

DESlock⁺[®]

protect your data.



DESlock+ is accredited with the following recognised approvals and standards.



FIPS-140-2

DESlock+ has been evaluated, tested and validated as compliant to the FIPS-140-2 standard under the Cryptographic Module Validation Program (CMVP) operated by NIST in the US and the Computer Security Division of the Canadian Government.



DIPCOG

The Defence Infosec Product Co-operation Group is a UK Ministry of Defence forum aimed to provide an interface between the MoD and IT security vendors DESlock+ (V3.2.7) is recommended by DIPCOG for MoD use.



CCTM

The Communications Electronic Security Group (CESG) Claims Tested Mark is a UK government standard for computer security products. Independent testing determines if a product meets the vendors claims. Successful products are awarded CCTM certification and become CESG certified products. V3.2.7

Certain features and functions of the DESlock+ software are protected by patents worldwide. Patent GB2378539, US7099478, US7471796, EU1423765, China ZL02820752.1, Israel 160709, Russia 2273959, India 231403 refers. Additional patents applied for.

DESlock+ is a Trademark of DESlock Ltd, and may not be used without their written permission. All other trademarks mentioned herein are property of their respective companies.

FIPS-120-2 Logo TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

Copyright © DESlock Ltd. (V4.4.147)

PLEASE READ THIS CAREFULLY BEFORE YOU INSTALL AND USE THIS SOFTWARE.

YOUR RIGHT TO USE THIS PRODUCT IS SUBJECT TO THE TERMS SET OUT BELOW. BY USING THIS PRODUCT YOU ARE ACCEPTING THESE TERMS.

1. DEFINITIONS

1.1 In this agreement the following words have the corresponding meanings:

"Agreement"	this software licence agreement;
"DESlock"	DESlock Limited (Co. No. 7875689) of Silver Street House, Silver Street, Taunton, Somerset, UK, TA1 3DL;
"Distributor" or "Reseller"	any third party authorised by DESlock to licence the product to third parties on behalf of DESlock;
"Documentation"	the user manual and any other documentation supplied as part of the software's help system;
"Information"	any information or data encrypted or decrypted using the software;
"IPR"	all intellectual property rights in the products (and any part of them) including without limitation the specific rights, any copyright, registered or unregistered trademarks, patents, database rights together with any applications to register the same anywhere in the world;
"Licence"	a non-exclusive, non-transferable licence to use the software and documentation in accordance with the terms of the agreement;
"Products"	the software and the documentation;
"Software"	the software(s) entitled DESlock+ used for the encryption and decryption of electronic data;
"Specific Rights"	the registered trademarks DESlock, DESlock+, patents GB 2378539, US 7099478, US 7471796, EU 1423765 (ES, FI, FR, UK, IE, IT, NL, DE, SE), RU 2273959, CN 02820752-1, IN 231403, IL 160709;
"Qualifying Personal User"	A person using the software solely in a personal capacity for personal data only, this includes full and part time students who use the software with any information related to their studies and research and any correspondence with their school, college or other institution or any other organisation which is involved in their personal training or education;

“Corporate Users”

Persons using the software with information belonging to a business or any other organisation of which the user is an employee or member of or is working for under any contractual or voluntary basis including working as self employed with the exception of correspondence directly relating to the single user such as personal contract of employment or correspondence relating to the terms and conditions of your employment.

- 1.2 All references to the plural shall include the singular and all references to the masculine shall include the feminine and neuter and vice versa.

2. GRANT OF LICENCE AND DESlock Ltd OBLIGATIONS

In consideration of you agreeing and adhering to the terms of this agreement, and paying for a licence, DESlock grants you a non-exclusive, non-transferable right to install and use the software for the number of Users for which you have purchased a licence. A separate licence is required for each and every User.

- 2.1 Qualifying personal users as defined in this agreement may use the personal edition of the software free of charge using the appropriate licence activation code provided by DESlock.
- 2.2 Corporate users as defined in this agreement are NOT permitted to use the software free of charge other than for initial trial and evaluation purposes or at the express permission of DESlock. See 3.2
- 2.3 With Corporate Site licences, the Licensee's User count may increase during the term of this License. The Licensee is not obligated to pay DESlock Limited for increased use during the Maintenance Period while the total number of Users does not exceed an amount greater than 10% above the Initial Number of Users. At the end of the Maintenance Period, if the Agreement is renewed then Licensee will pay the new Licence fees for the added Users and Licensee will pay the renewal maintenance fees for the remaining Users. If the total number of Users has increased by more than 10% during the Maintenance Period, then the Licensee will pay DESlock Limited the new license fees before such Software is used and based on DESlock Limited's current license fees.

3. PERMISSIONS

Subject to this agreement you are permitted to:

- 3.1 Load and use the software on one or more computers for your own use (in object code form only) in conjunction with the licence activation code;
- 3.2 Licensed Corporate Users may load and use the software on one or more computers (in object code form only) in conjunction with the licence activation code. Licensed Corporate users may also load and use the software on home computers (personal use) but without Full Disk Encryption.

- 3.3 Make a back-up copy of the software in support of your permitted use of the software provided you clearly label the back-up copy with the following notice:

© DESlock Limited – All rights reserved
- 3.4 Use the documentation for the purpose of providing you with assistance on the use of the software;
- 3.5 Transfer the products and your licence on a permanent basis to another person only if that person agrees to accept the terms of this agreement and you either transfer all copies (including the most recent update and all prior versions) to that person or destroy any copies not transferred. If you transfer possession of any part of the products to another person, your licence is automatically terminated.

4. PROHIBITIONS

You may not nor may you permit others to:

- 4.1 Use the software in a corporate environment or in conjunction with any information relating to a business other than your own personal data unless licensed to do so by DESlock.
- 4.2 use, copy, distribute, rent, loan, lease, sub-licence, transfer or otherwise deal in the products (or any of them) except as permitted by this agreement;
- 4.3 alter, adapt, merge, modify or translate the software or the documentation in any way for any purpose, including, without limitation, for error correction except with express prior permission of DESlock (which may be withheld at its absolute discretion);
- 4.4 reverse – engineer, disassemble or decompile the software, activation code or software key file;
- 4.5 remove, change or obscure any identification or notices of proprietary rights (including without limit those relating to the specific rights) and restrictions on or in the products (or any of them).

5. TERMINATION

- 5.1 You may terminate the licence at any time by deleting all electronic copies of the software in your control together with any back-up disks and returning the products together with all copies in any form to DESlock or the distributor or reseller from which you purchased the same. Any use of any copies of the products after termination of the licence is unlawful.
- 5.2 Your licence to use the products will terminate automatically if you:
 - 5.2.1 fail to comply with any term of this agreement; or

- 5.2.2 become bankrupt, go into liquidation, suffer or make any winding up petition, make an arrangement with your creditors, have an administrator, administrative receiver or receiver appointed or suffer or file any similar action.
- 5.3 Upon termination of the licence for any reason you will delete all electronic copies of the software in your control together with any back-up disks and return the products together with all copies in any form to DESlock or the distributor or reseller from which you purchased the same. Any use of any copies of the products after termination of the licence is unlawful.

6. LIMITED WARRANTY

- 6.1 Subject to clause 6.2 and clause 8.4 DESlock warrants only to you as the original licensee that for a period of 12 months from the date upon which you purchased the products, the software, when used properly, will in all material respects provide the functions and facilities as described in the documentation.
- 6.2 DESlock's entire liability and your exclusive remedy under the warranty given in clause 6.1 will be (at DESlock's absolute option) to either:
 - 6.2.1 repair or replace the products (if any) which does not conform with the warranty; or
 - 6.2.2 refund the price paid for the products and terminate the Licence. This remedy is subject to the return of the products with a copy of your payment receipt to DESlock not later than 14 days after the end of a period of 12 months from your purchase of the software.

7. EXCLUSION OF OTHER WARRANTIES

- 7.1 Subject to the express warranties given pursuant to clause 6, DESlock make and you receive no other warranties, conditions or representations, express or implied, statutory or otherwise, and without limitation the implied terms of satisfactory quality and fitness for a particular purpose are excluded. DESlock does not warrant that the operation of the products will be error free or uninterrupted. It is your responsibility to ensure that the products are suitable for your needs and the entire risk as to the performance and results of the products is assumed by you.
- 7.2 You acknowledge and accept that:
 - 7.2.1 it is your responsibility to protect, maintain and back-up Information;
 - 7.2.2 you should fully back-up all information and data (including without limit any critical information and data) on your computer **before** installation of the software;

- 7.2.3 you **must** keep a safe record of any passwords or other information used for setting up and using the software, you **must** also make backup copies of all encryption keys, licence codes, key-files and other data generated to separate storage media;
- 7.2.4 you are responsible for the use of the products. DESlock shall not be liable for any loss, claim or damage suffered as a consequence of any unauthorised or mistaken encryption or decryption of information or data (including without limit, information) wherever and however that information or data is stored;
- 7.2.5 whilst DESlock has taken all reasonable steps to ensure the integrity and security of the software, the products (or any of them) must **not** be used in any area which is dependent on a fail-safe level of security or is potentially hazardous or dangerous including without limitation nuclear facilities, aircraft navigation, control or communication systems, weapon and defence systems and life support or life monitoring systems;
- 7.2.6 it is your responsibility to ensure that the level of security and encryption provided by the products is adequate for your requirements;
- 7.2.7 you are responsible for your use of the products (or any of them) including without limit ensuring that such use complies with all applicable laws and regulations of the United Kingdom or such other country, region or state where the product is used. You must ensure that prior to any use of the products you have ensured that it is not in contravention of any government (in the United Kingdom or otherwise) embargo;
- 7.2.8 It is your responsibility to keep safe records of any information used for setting up and using the software. You **must** keep a safe record of any passwords or other information used for setting up and using the software. You **must** also make backup copies of all encryption keys, activation codes and other data generated to separate storage media;
- 7.2.9 DESlock shall not be responsible for any loss, damage, expense or claim arising from the loss, theft, misuse, corruption, damage or destruction of passwords, set up information, encryption keys, licence activation codes and other data generated or stored during use of the software.

8. DISCLAIMER

- 8.1 Notwithstanding anything to the contrary in this agreement DESlock does not exclude or limit liability for death or personal injury resulting from an act or negligence of DESlock.

- 8.2 DESlock will not be liable for any direct, consequential, incidental, or special damage or loss, damage or claim of any kind (including without limitation loss of profits, loss of contracts, business interruptions or loss of, unauthorised or mistaken disclosure or corruption to Information and / or data) however caused and whether arising under contract, tort, including negligence, or otherwise in respect of the products and your use of them (including without limit any “beta” product provided pursuant to clause 8.4 below).
- 8.3 If any exclusion, disclaimer or other provision contained in this agreement is held invalid for any reason and DESlock becomes liable for loss or damage that could otherwise be limited, such liability, whether in contract, negligence or otherwise, will not exceed the amount actually paid by you for the products.
- 8.4 Any products (including any supporting software, data or information) supplied by DESlock or its distributors or resellers as a “beta” product are provided “as is” and are to be used for evaluation purposes only. Under **no** circumstances should any “beta” product provided pursuant to this clause be used in conjunction with any confidential, critical or important information or data;
- 8.5 You acknowledge that the allocation of risk in this agreement is fair and reasonable in all the circumstances and that it is not within DESlock control how and for what purposes the products are used by you.

9. INDEMNITY

You will fully indemnify DESlock against any loss, damage, expense (including without limit any legal fees) or claim incurred as a consequence of you failing to adhere to any of the terms of this licence.

10. GENERAL

- 10.1 This agreement is the entire agreement between you and DESlock and supersedes any other oral or written communications, agreements or representations with respect to the products.
- 10.2 If any part of this agreement is held by a court of competent jurisdiction to be unenforceable the validity of the remainder of the agreement will not be affected.
- 10.3 This agreement is governed by the laws of England and Wales and the parties submit to the exclusive jurisdiction of the English court.
- 10.4 Except as otherwise expressly stated herein, nothing in this agreement confers any rights on any person (other than the parties hereto) pursuant to the Contracts (rights of third parties) Act 1999.

- 10.5 The waiver by DESlock of any breach or failure to enforce any of the terms and conditions of this agreement at any time shall not in any way affect, limit or waive DESlock' rights thereafter to enforce and compel strict compliance with every term and condition of this agreement.

11. ADDITIONAL RIGHTS FOR CONSUMERS

The following provisions are applicable if you are purchasing the products as a consumer and by means of a distance contract. For the purpose of this clause '*consumer*' and '*distance contract*' shall have the same meaning as set out in the Consumer Protection (Distance Selling) regulations 2000.

- 11.1 The price paid for the products includes the cost of delivering the same to you and all applicable taxes.
- 11.2 The price must be paid in full before the products are despatched to you. DESlock will use its reasonable endeavours to deliver the products to you within 14 days from the date of payment.
- 11.3 Notwithstanding anything to the contrary in this agreement, you have the right to cancel this agreement at anytime within 7 working days from the date you receive the products. Should you exercise your right to cancel pursuant to this clause you should immediately return the products unused, undamaged and fully intact by recorded delivery to DESlock (at the address set out at in clause 1.1 ('DESlock') of this agreement). You are responsible for the cost of returning any products no longer required pursuant to this clause. DESlock will refund any monies paid by you to DESlock within 14 days of receipt of the products in accordance with this clause (or within 30 days from the date of such cancellation whichever is the earlier).
- 11.4 If you have any complaints about the products or DESlock these should be reported in writing to:
- Quality Manager
DESlock Limited
Silver Street House
Silver Street
Taunton
Somerset, UK
TA1 3DL
- 11.5 DESlock gives no guarantees, warranties or after sales service other than as set out in this agreement.
- 11.6 Nothing in this agreement will affect the statutory rights of a consumer in 'consumer transactions' under any applicable statute.

Getting Started

What is DESlock+?

DESlock+ is a feature-rich Windows data encryption utility capable of encrypting hard drives, folders, files, data and emails. Entire disks can also be encrypted using Full Disk Encryption or Removable Media Encryption (subject to appropriate product licence).

Files can be encrypted individually or as the content of an encrypted folder, drive or compressed archive. Email messages can be encrypted directly from the Outlook plug-in, or from the Windows Clipboard.

The DESlock+ Shredder provides secure drag and drop file deletion with the additional option to securely delete the contents of the recycle bin, temporary files, Internet explorer history and other information with just a mouse click.

In a corporate environment DESlock+ can be managed using the DESlock+ Enterprise Server software. This allows complete remote management of encryption features and policy for individual workstations and users. Encryption policy can be enforced and encryption keys issued and revoked keeping data secure and preventing loss and leakage of sensitive information.

DESlock+ can also be used in standalone mode with all licenced features available to the user

How does it work?

DESlock+ encrypts data using either an encryption key which is stored in a secure Key File, or using a user generated password or pass phrase. Encryption keys are used in conjunction with trusted industry standard encryption algorithms to encrypt the data to be secured. Encryption keys are unique so data encrypted with a particular key can then only be decrypted with that same key.

Up to 64 different encryption keys can be generated and stored and are then available once the user is logged into DESlock+ by entering a user defined password or phrase. The number of keys that can be stored depends on the product licence type.

Encryption keys can easily be issued and transferred securely between DESlock+ users using a public / private key exchange process with no restriction on the number of users. This allows encrypted data to be accessed and shared by multiple users provided they have the appropriate encryption key.

The generation and management of encryption keys is controlled using protected settings within the users Key File. Encryption keys can be generated, shared and backed up by the user. In addition unique, patented, key propagation methods make it possible to control the range and scope of key sharing within a workgroup.

The DESlock+ software has a number of industry accreditations and approvals it also incorporates a FIPS 140-2 certified cryptographic core which uses the highly secure 256-bit AES algorithm for encrypting data.

DESlock+ user types

There are two main types of DESlock+ users, Managed and Unmanaged.

Managed User. A Managed User is one who is under the full control of an Administrator. The Administrator controls which DESlock+ functions the user has access to and can impose a wide range of operational policy onto that user. A Managed User may not have access to all the functions described in this manual.

Unmanaged User. An Unmanaged or Stand alone user has full control of all the options, features and usages of DESlock+, depending on licence type (Standard or Pro) purchased.

For more information on DESlock+ user types see [Managed and Unmanaged users](#)

System Requirements

DESlock+ requires a minimum specification of machine in order to run effectively. The system should comply with or exceed the specifications listed below:

Operating System.

- Microsoft Windows XP, Vista, Windows 7 and 8 - 32bit or 64bit.
- Windows Server 2003 32bit.
- Windows Server 2008 64bit.

DESlock+ 64bit can be installed on Server 2008 R2 with Remote Desktop Services, allowing remote users access to core DESlock+ features such as Outlook Email Encryption, Encrypted Archives, Encrypted Files and Encrypted Virtual Disks.

Other requirements

- 64MB of hard-disk space
- 128MB of RAM
- Internet Explorer 6 or later
- Internet Access required for the Licence Wizard.

- Windows XP requires Service Pack 3, this is available from Microsoft.

Important note:

Installing DESlock+ on a machine which has Terminal Services installed, MUST be installed from the Add/Remove Programs applet in the Control Panel. Failure to do this will result in DESlock+ not working.

Encryption Algorithms

DESlock+ supports three algorithms to perform encryption of files and folders. The Key Generation Wizard allows the algorithm type to be selected from the following:

3DES

3DES (Triple DES) is a variant form of the DES (Data Encryption Standard) algorithm, originally developed by IBM in 1974. 3DES uses 2 56-bit keys, giving an effective key length of 112 bits, and performs DES encryption on the data three times using these keys.

Blowfish

The Blowfish algorithm was developed in 1993 by Bruce Schneier, President of a consulting firm specialising in computer security, and author of Applied Cryptography. Blowfish is a 64-bit block cipher with a single 128-bit encryption key.

AES

AES (Advanced Encryption Standard) was developed as a new encryption standard to replace DES. Rijndael was accepted as the AES algorithm on October 2, 2000. The Rijndael algorithm was developed by Joan Daemen and Vincent Rijmen, Belgian cryptographers who gained PhDs at the computer security and industrial cryptography labs at Universiteit Leuven. DESlock+ supports AES with a key length of up to 256 bits.

Key Exchange Algorithm

DESlock+ also uses the RSA algorithm and Public Key cryptography techniques for all key transfer operations. This allows encryption keys to be securely transferred even via insecure communication channels e.g. the Internet.

RSA

The RSA asymmetric algorithm was named after Ronald Rivest, Adi Shamir and Leonard Adelman, Computer Science researchers at the Massachusetts Institute of Technology, who developed and patented the algorithm in 1977.

Full Disk Encryption

Full Disk Encryption uses a FIPS 140-2 certified AES 256 algorithm.

Quick Start Guide

Managed Users

If you are working in a managed environment you will have been provided with an MSI installation package and an activation code by your systems administrator, either as a file or on a CD. This package contains specific policy settings for you as a user and for your workstation. Managed users should refer to their systems administrator for updates if required. Software or activation codes downloaded from the DESlock+ Website will not install or function over a managed installation

If you are working in a managed environment where DESlock+ is controlled by the DESlock+ Enterprise Server software please see [Login to DESlock+ - Managed Users](#) in the main manual.

Unmanaged (standalone) users

To use DESlock+ you need to install the software and obtain an Activation Code. See below for details.

To Download DESlock+

1. Go to www.deslock.com/login.php
2. Register using your valid email address and your chosen password to gain access to the DESlock+ website in the future. Answer the questions with the drop down boxes and click 'Register'. You will receive a confirmation and account validation email at your registered email address.

DESlock+ Protect your data. LOGIN/REGISTER

HOME PRODUCTS DOWNLOADS SOLUTIONS SUPPORT NEWS CONTACT STORE PARTNERS

Login

Email:
Password:
Forgotten Password? Click here.

To purchase a licence/voucher or view an existing licence/voucher please login. If you have not yet registered then please use the form to the right.

Your personal information

i Any information you supply to us for this purpose will never be disclosed or sold to third parties or marketing firms and will only be used by ourselves or our distribution and resale partners in connection with our products and services.

Following registration you will receive a confirmation email which will allow you to activate your DESlock+ online account. If you do not appear to have received an email, please first check your junk-email folder.

Register

All Users:

Email: Password:
Confirm Email: Confirm password: * - Required field

Business Users:

Trial period support:
If you are evaluating DESlock+ for 25 users or more, we will provide telephone/email support during your trial period.
Number of users:
☐ Free telephone/email support

Product Features Required:
☐ Removable Media Encryption
☐ Full-Disk Encryption
☐ File & Folder Encryption
☐ Email Encryption
☐ Enterprise Server
☐ Other
Please choose at least one *

Multi-user pilot scheme:
If you are using this licence to evaluate our software for business use, and would like information about our multi-user pilot scheme, please check the box below.
For qualified enquiries requiring 100 users or more, we are offering our Enterprise Server and ten DESlock+ Pro or Standard licences free of charge.
These are not trial licences and will allow you to undertake a live, multi-user evaluation. This is a limited offer, so contact our sales team today and register your enquiry.
☐ Please contact me to discuss a managed multi-user evaluation

Your Information:
Title:
First name:
Last name:
Job or Role:
Company:
Industry:
Country:
* - Required field for:
- Email/Telephone Support
- Multi-user Evaluations
- Enterprise Server Evaluations

☐ I accept the terms of the DES privacy policy: *

3. Once you have received your validation email click on the Validation link (or cut and paste it into your browser) this will then give access to the Download Area.

4. In the Download Area Select the licence type you require by clicking on the link, your activation code will appear in the next window.

The different licence types available are shown below along with the feature set for each type:

Licensing			
DESlock+ is a common install, the licence type defining the feature set, Licence upgrades enable additional features seamlessly.			
	Personal (Free)	Standard	Pro
Full Disk Encryption			✓
Removeable Media Encryption		✓	✓
DLP Go Portable Encryption		✓	✓
File & Folder Encryption	✓	✓	✓
Outlook Email Encryption	✓	✓	✓
Virtual Disks and Archives	✓	✓	✓
Text and Clipboard Encryption	✓	✓	✓

By clicking on the links within the 'Your Licence' window (see below) you can select one of the following:

- Purchase a full licence direct from the DESlock+ Website or one of our Resellers.
- Get a **free** trial licence for a fully functional version of DESlock+ Standard or Pro .
- Get a **free** Personal Licence.
- Redeem a promotional code.

Your Licence

You do not have a licence.

To obtain a Licence please choose one of the following:

- You can purchase a Full Licence online now.
 - To purchase from a reseller please [click here](#)
 - To purchase direct from this website [click here](#)
- Get a Trial Licence:
 - [click here for a Standard Trial](#)
 - [click here for a Pro Trial](#)
- Get a Free Personal Licence:
 - [click here to request a Free Personal Licence](#)
- If you have a promo code, use it here:

- -

30 character code

10 character code

5. Once you have selected your licence type and accepted the terms and conditions your Activation code will be displayed on the Web page, together with a download link for the software. Download the correct type for your Operating System (32 or 64 bit)

Your Licence

Registered to:	sample@email.com
Type:	Personal Edition
Registered Date:	22 Sep 2011
Duration:	Full Licence

Your Activation Code
 NNNNN - NNNNN - NNNNN - NNNNN - NNNNN

You will be asked for this activation code during installation.

• If you have a promo code, use it here:

30 character code

(Having trouble finding your code?)

10 character code

Your Downloads

Download DESlock+

32-bit DOWNLOAD

Version:

4.3.68 (32-bit)

64-bit DOWNLOAD

Version:

4.3.68 (64-bit)

Minimum System Requirements

DESlock+ requires a minimum specification of machine in order to run effectively. The system should comply with or exceed the specifications listed below:

32-bit and 64-bit versions of the following operating systems

- Windows 7
- Windows Vista
- Windows XP *
- Windows Server 2008 (64-bit only)**
- Windows Server 2003

- Pentium 300MHz
- 128MB of RAM
- 64MB of hard-disk space
- Internet Explorer 6 or later

For more information about this release, please read the [Release notes](#).

* Windows XP requires Service Pack 3, this is available from Microsoft

** DESlock+ 64bit can also be installed on Server 2008 R2 with Remote Desktop Services, allowing remote users access to core DESlock+ features such as Outlook Email Encryption, Encrypted Archives, Encrypted Files and Encrypted Virtual Disks.

If you wish to download DESlock+ 3.2.7 or require CCTM approved software, please [contact us for further details](#)

6. Click on the 'Download DESlock+' link to download the software.
7. Install the software. Start the installation by double clicking the downloaded file, and follow the steps, providing information as needed.
8. Alternatively, you may have been provided with an MSI software installation package or a CD containing the software, if so follow the instructions provided with it.
9. The last action for the installation is a system restart. When the computer has restarted, the DESlock+ login screen will be displayed as below. Click 'Setup'

DESlock+
protect your data.

Select the item you wish to activate from the list below.

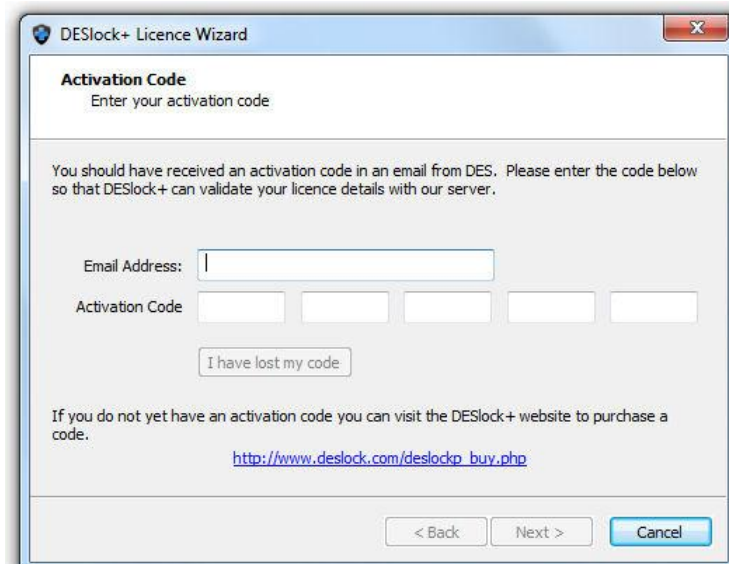
Enter your user password and click ok.
Alternatively, if the item has not been configured click setup.

Name	Serial Number	Comment
My Key-file	80000001	Double click to launch key setup

The Key-File must be setup before you can login to DESlock+

Choose 'Setup' or 'Restore' from a backup.

10. To use DESlock+, you need to configure your Key-File. The Key-File is a bit like a key-ring and is where your encryption keys will be securely stored. Encryption keys are used for encrypting your data and you can create different keys to protect different types of data, or perhaps create keys to share your encrypted data with others.
11. Click 'Setup' on the Login window, this will start the Licence Wizard. Click 'Next' and the Activation window will display.



12. Open your browser; navigate to the DESlock+ Website and login to your account. Copy the Activation code from the left hand panel. This activation code will also have been sent to your registered email address and can also be copied from there. Alternatively, you may have a 30 or 10 character Promotional Code, if so enter the code in the spaces provided on the webpage. Once you have entered the Activation Code into the Licence Wizard, click 'Next'.

Your Licence

Registered to:	sample@email.com
Type:	Personal Edition
Registered Date:	22 Sep 2011
Duration:	Full Licence

Your Activation Code
NNNNN - NNNNN - NNNNN - NNNNN - NNNNN

You will be asked for this activation code during installation.

If you have a promo code, use it here:

- - **USE**

30 character code

USE (Having trouble finding your code?)

10 character code

Your Downloads

Download DESlock+

32-bit DOWNLOAD
Version: 4.3.68 (32-bit)

64-bit DOWNLOAD
Version: 4.3.68 (64-bit)

Minimum System Requirements
DESlock+ requires a minimum specification of machine in order to run effectively. The system should comply with or exceed the specifications listed below:
32-bit and 64-bit versions of the following operating systems

- Windows 7
- Windows Vista
- Windows XP *
- Windows Server 2008 (64-bit only)**
- Windows Server 2003

- Pentium 300MHz
- 128MB of RAM
- 64MB of hard-disk space
- Internet Explorer 6 or later

For more information about this release, please read the [Release notes](#).

* Windows XP requires Service Pack 3, this is available from Microsoft
** DESlock+ 64bit can also be installed on Server 2008 R2 with Remote Desktop Services, allowing remote users access to core DESlock+ features such as Outlook Email Encryption, Encrypted Archives, Encrypted Files and Encrypted Virtual Disks.

If you wish to download DESlock+ 3.2.7 or require CCTM approved software, please [contact us for further details](#)

DESlock+ Licence Wizard

Activation Code
Enter your activation code

You should have received an activation code in an email from DES. Please enter the code below so that DESlock+ can validate your licence details with our server.

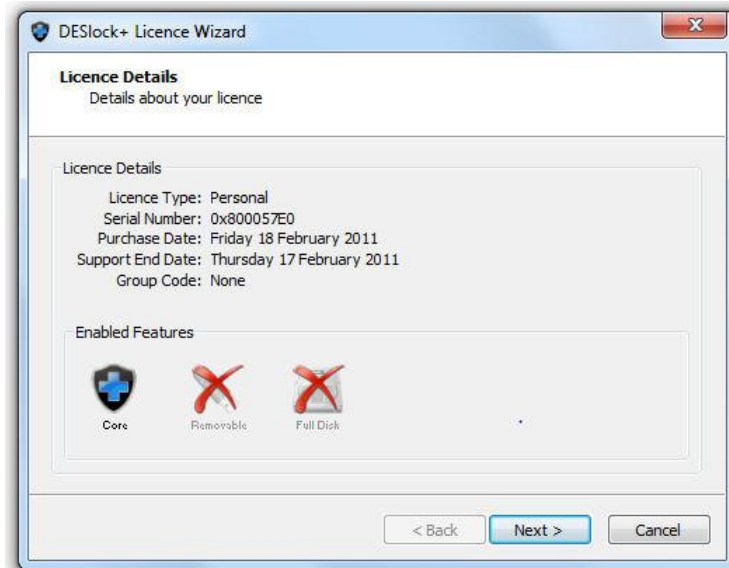
Email Address:

Activation Code

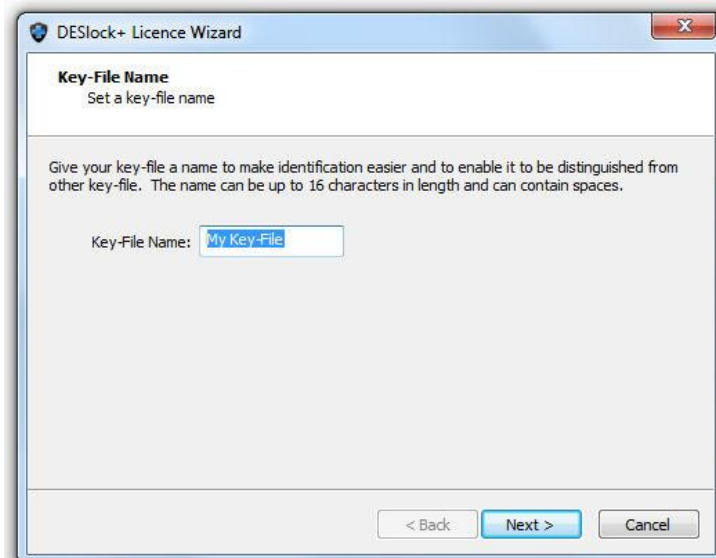
I have lost my code

If you do not yet have an activation code you can visit the DESlock+ website to purchase a code.
http://www.deslock.com/deslockp_buy.php

13. The next window displays the licence type you have installed, and the features that are enabled. The example shown is for a Personal Licence with Removable Media and Full Disk Encryption being unavailable.



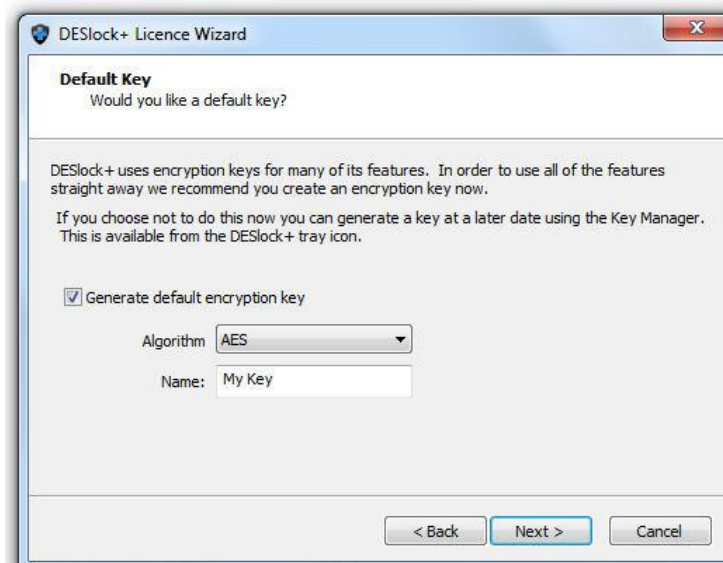
14. Give your Key-File a unique name to allow easy identification.



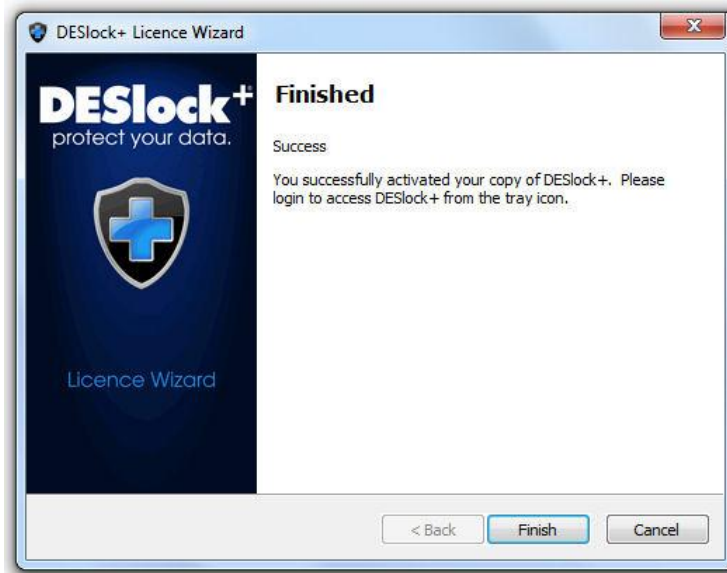
15. To login to DESlock+ and your Key-File you will require a password. The next stage is to set this password. Make sure you use a password that is unlikely to be guessed by somebody else and be sure to make a note of it in a secure place. You must enter your chosen password twice, the second time to confirm the entry: The 'next' button will not be available if the 'Confirm' password does not match the first, you can select the 'show typing' tick box to verify that the text is the same - passwords are case sensitive. **Note.** This is a new password and not the one you used to register your account at www.deslock.com



16. You can now generate your first Encryption Key, known as your default Encryption Key. Ensure the 'Generate default encryption key' box is checked, select the desired algorithm type and enter a name for the encryption key. For more information about encryption keys and algorithm types please see the [Technical Information](#) section. You can generate additional encryption keys at any stage in the future using the DESlock+ Key Manager.



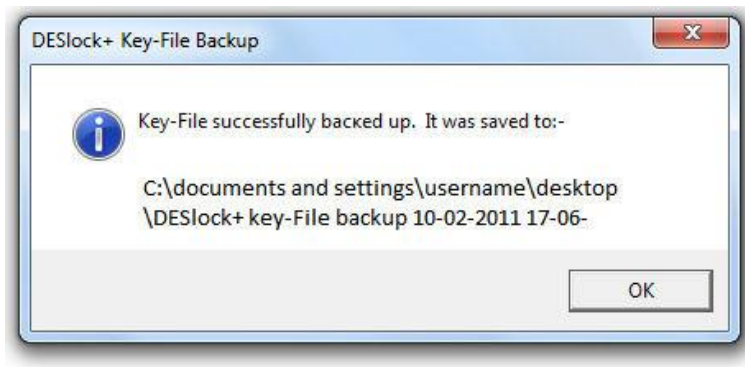
17. Once all the information has been entered, click 'Next' and the wizard will finish.



As every encryption key generated is entirely unique, your Key-File, which contains your keys, must be backed up to a secure location, ideally a memory stick, network drive or external hard drive separate to your computer. Should all copies of your Key-File and encryption key be lost it will not be possible to decrypt any data you have encrypted with them, so this is very important.

18. The Key-File backup feature will run automatically. If, at any time, you add encryption keys to your Key-File this backup will run. Using the 'Browse' button, define a location for the key file backup and click 'OK'. If the location chosen is on the same drive as the current Key-File, you will get a warning message as a separate drive or removable media is recommend. Once complete the backup wizard will display the backup file name and location. **WARNING - VERY IMPORTANT. Do not save the key file backup to any location that is encrypted with a key (or that you will encrypt with a key in future) - if you need to restore your backup this will not be possible if the backup location is encrypted. If you must encrypt your backup do so with a Password that you will not forget.**





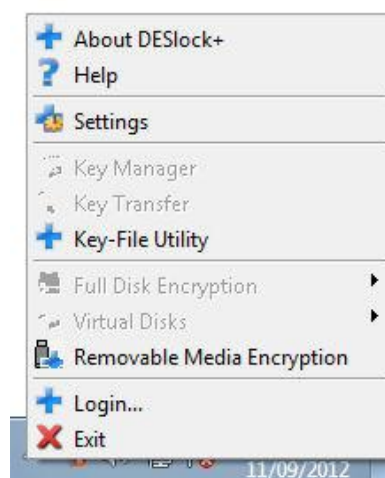
19. You can now log into DESlock+ for the first time. DESlock+ will initially be disabled, denoted by the flashing status icon, a grey cross, in the System Tray (see below).



20. **Important** - Windows 7 users take note. By default, on Windows 7, any new system tray icons (such as DESlock+) are hidden shortly after being installed. To view any hidden icons simply click the up arrow next to the other system tray icons and click as shown in this picture. Login to DESlock plus as described in the next step. Click here for more information on [Windows 7 System tray](#) icons and how to modify their behaviour.

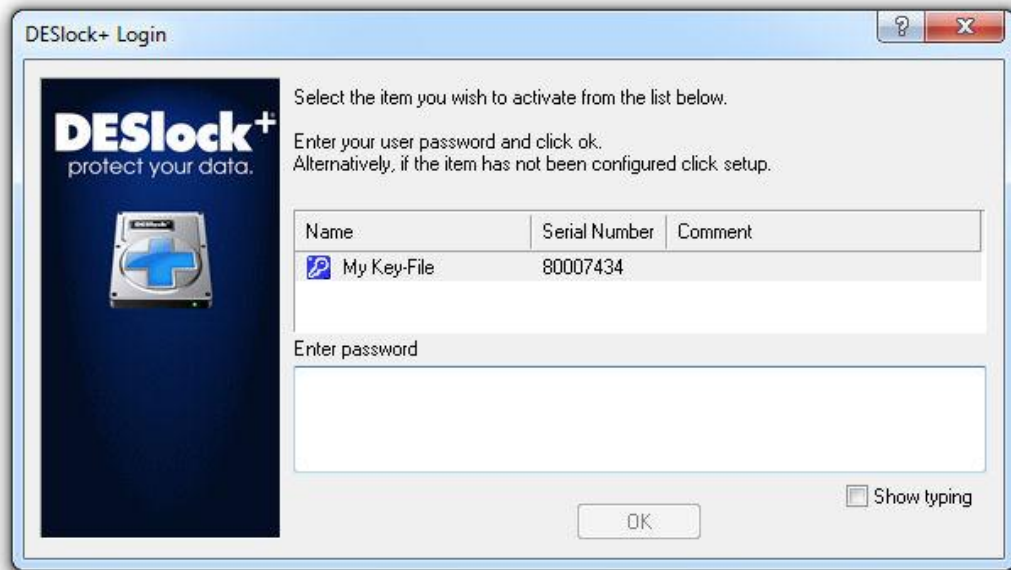


21. Right click the DESlock+ status icon in the System Tray and select 'Login' (see below).



22. The DESlock+ Login box will now be displayed. Enter the correct password and click

'OK'. Note - this is the Key-File password you entered at stage 15 above.



23. The DESlock+ icon in the System Tray will change to a blue cross (enabled).



DESlock+ is now ready for use

For advice on how to protect your data please read the chapter on Basic Encryption in the DESlock+ Help file or the User Manual.

Windows 7 System tray

By default on Windows 7, any new system tray icons (such as DESlock+) are hidden shortly after being installed. To view any hidden icons simply click the up arrow next to the other system tray icons and clock, as shown below.



To access DESlock+, right click on the blue (or grey) DESlock+ symbol.

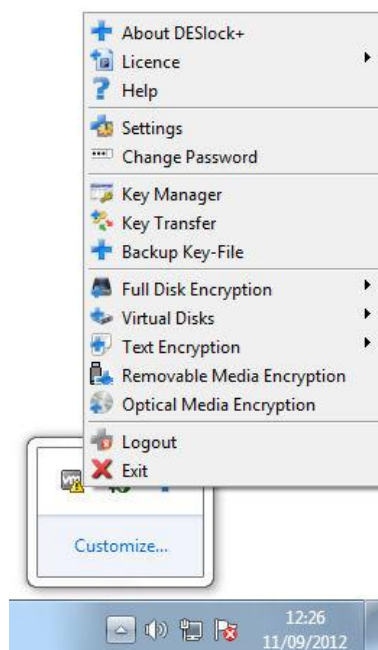


DESlock+ Logged on.

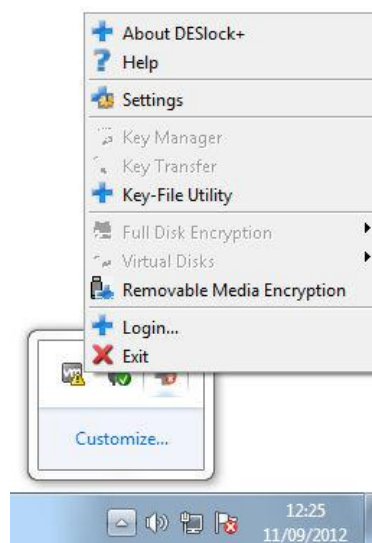


DESlock+ not Logged on.

This will display the DESlock+ system tray menu, giving you access to the features of DESlock+ available on your licence. If you are not logged into DESlock+ you will only have access to certain functions. To use these functions please refer to the rest of this manual.

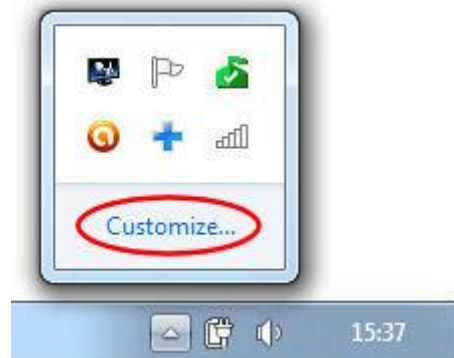


DESlock+ Logged on.

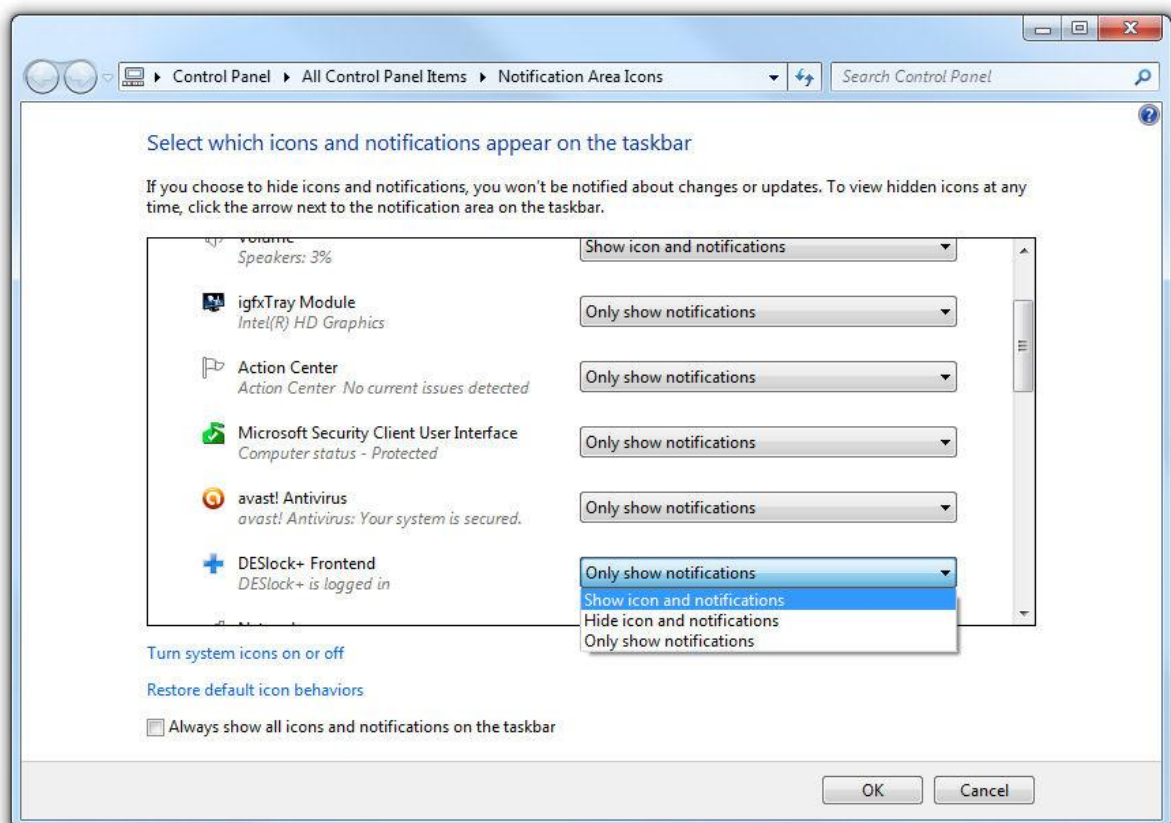


DESlock+ not Logged on.

If you wish to change the DESlock+ Icon to display permanently in the system tray, you need to change its properties. To do this click the 'Customize' option.



This will display the 'Notification Area Icons' control panel. Scroll down the list until you find the DESlock+ Front-end entry. Change the 'Behavior' from 'Only show notifications' to 'Show icon and notifications'.



Click 'OK' and the DESlock+ Icon will display in the System Tray, as shown below.



Basic Encryption

DESlock+ is a feature rich data encryption utility which can be used to encrypt complete hard disks, removable media, folders, individual files, sections of text plus emails and attachments. It can also be used to create virtual encrypted disks, encrypted file archives and also has the ability to securely delete data so that it cannot be retrieved.

Each of the basic encryption functions are described below. From each subject you can link to the relevant section for a full description and step by step guide to using each feature.

The features available are controlled by the software licence (via an activation code). If you are working in a managed environment the features available to workstations and users are controlled by the system's administrator via the DESlock+ Enterprise Server software.

Full Disk Encryption

With full disk encryption the entire capacity the computer's hard drive will be encrypted. This will include all the data and programs stored on it. Once the initial process of encrypting the hard drive has been completed a user will need to login to the computer when it is first switched on, known as pre-boot authentication, using a password. Once logged on the computer will operate as normal with all data and programs being available. However, the computer cannot be accessed without the login password. Full disk encryption therefore gives the best protection of data stored on a portable device as if it were stolen it would be impossible to access the data without the correct password. If the hard disk was removed and used with another computer the contents of the disk would still remain encrypted and completely inaccessible.

For a quick guide see the [Full Disk Encryption - Quick Guide](#) section.

For a 'how to' guide see the [Full Disk Encryption](#) section in the main manual.

Folder Encryption

With folder encryption the contents of a folder, including any sub-folders, is encrypted. Any new files or folders created within the folder will also be encrypted. If you drag and drop in a file or folder it will be encrypted and if you drag out a file or folder it will be decrypted. Provided that you are logged into DESlock+ files within an encrypted folder will open and save as usual. If you are not logged into DESlock+, the files within the folder will remain encrypted and programs will either not be able to access the files, not be able to recognize them, or the files will open but will show encrypted data. DESlock+ can be set to hide all encrypted folders when not logged in so they are invisible to DESlock+.

For a quick guide see the [Folder Encryption - Quick Guide](#) section.

For a 'how to' guide see the [Folder Encryption](#) section in the main manual.

File Encryption

With file encryption a single file is encrypted. To be able to access the file you will need to decrypt it. This method is often used to secure files while they are transferred by email, CD/DVD, memory card / stick etc.

For a quick guide see the [File Encryption - Quick Guide](#) section

For a 'how to' guide see the [File Encryption](#) section in the main manual.

Virtual Disks

DESlock+ can be used to create a virtual disk drive that is encrypted. When the file is 'mounted' (accessed through DESlock+) it will appear and function as an additional hard disk on your computer. As with folder encryption, any files and sub folders on the virtual drive will be encrypted, as will any files added to the virtual drive. Anything removed from the drive will be automatically decrypted.

For a quick guide see the [Virtual Disks - Quick Guide](#) section

For a 'how to' guide see the [Virtual Disk Manager](#) section in the main manual.

Encrypted Archives

An encrypted archive is similar to a Zip file – it's a method of compressing data (one or more files or folders) to save disk space, but with the added bonus that the data is encrypted. Again, as you add or remove files they are automatically encrypted or decrypted. When the archive is opened, you can use the files within it normally.

For a quick guide see the [Encrypted Archives - Quick Guide](#) section

For a 'how to' guide see the [DESlock+ Archive](#) section in the main manual.

The different methods of encryption have their advantages and disadvantages. Full disk is easiest of all to use and is the most secure, but, everything on your computer is encrypted - you forget your password (and the admin password) and you cannot run your computer. Folder encryption is simple to use, but the unwary could leave plain data available, as it relies on you always saving to a specific folder. File encryption is good for transferring data by email or memory device, as are archives, but both require user action. Virtual Disks (and archives) are very secure, as they appear as a single block of encrypted data with no discernible files.

Encryption keys and Key-Files

Keys

Encryption of data is performed through the use of encryption keys. The key is used to scramble the data in such a way that it can only be unscrambled using that same key. You can keep the only copy of a key, or you can share it with others, as many times as you like. If you share a key, any holder of that key can decrypt any data you have encrypted with it.

Key-Files

Each key is kept in a Key-File (a bit like a key ring). Key-Files can hold several keys (up to 64, depending on your licence type). While a single user may only need one key, any environment where you have a requirement to share data securely with another user, you may need more than one key. The Key-File allows you to have a single place where your keys are kept.

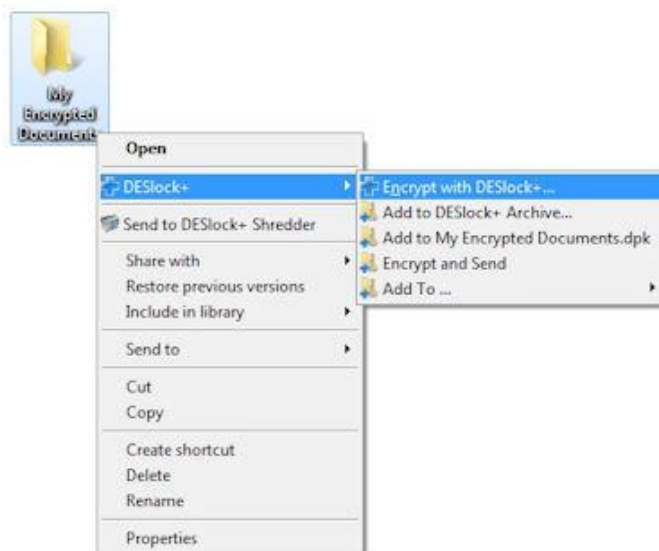
Full Disk Encryption - Quick Guide

Full Disk Encryption **should not be attempted** without first making a complete backup of your disk. Essentially the process will encrypt every bit of information on your Hard disk, but in a way that allows you to continue working. It will take a reasonable amount of time to complete, dependant on disk size and system speed. For full details of the process see the [Full Disk Encryption section](#) in the main manual. Full Disk Encryption is only possible if that option is included on your licence. The basic standalone (Unmanaged) process is outlined below.

- To begin the encryption process, run the DESlock+ Full Disk Tool from the system tray menu.
- Then click the Disk Management button.
- Select the disk and/or partitions you wish to encrypt using the selection boxes
- Record the Administrative password securely, using the 'Save to file' button. If you lose this you will not be able to decrypt your disk at a later date.
- Provide your own username and password. This will be used to access the Disk each time the system is switched on.
- The encryption process will start, and continue in the background until it is completed. You can use the machine as normal during the encryption process, even shutting the system down and rebooting. Next time you Boot your system, even if the encryption has not completed, you will have to enter the correct username and password, before windows starts.

Folder Encryption - Quick Guide

Any folder (except system folders) can be encrypted with DESlock+ by right clicking on them, select DESlock, then Encrypt with DESlock+.



You will have to then select the Encryption key to use, and verify that you have backed up your data. DESlock+ will then encrypt the folder and all its contents (including any sub-folders). Before completion you can select if you want the plain copy left or deleted. See [Folder Encryption](#) in the main manual for more details.

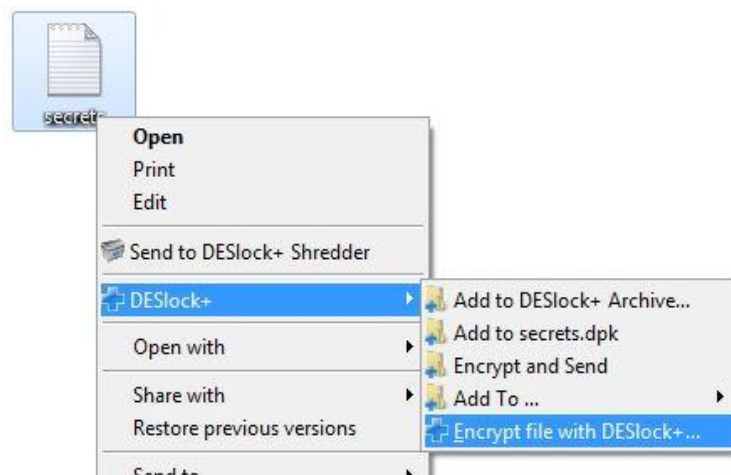
Once encrypted the folder icon changes (see below) and any file that you place in that folder is automatically encrypted - and automatically decrypted when you move it out of the folder. You can use the folder as normal - for example, double click on a file in the folder and it will open as normal using the correct program.

Note - some programs create their own copies of open files in temporary folders while you are using them. It is your responsibility to ensure that these copies do not compromise your security. (Use the DESlock+ shredder to clean these folders out)



File Encryption - Quick Guide

Any file (except system files) can be encrypted by right clicking on them. Select 'DESlock+', then "Encrypt file with DESlock+", from the context menu that appears. (See below). As with Folder Encryption (and any encryption process) you will have to select the encryption key to use in the window that follows.



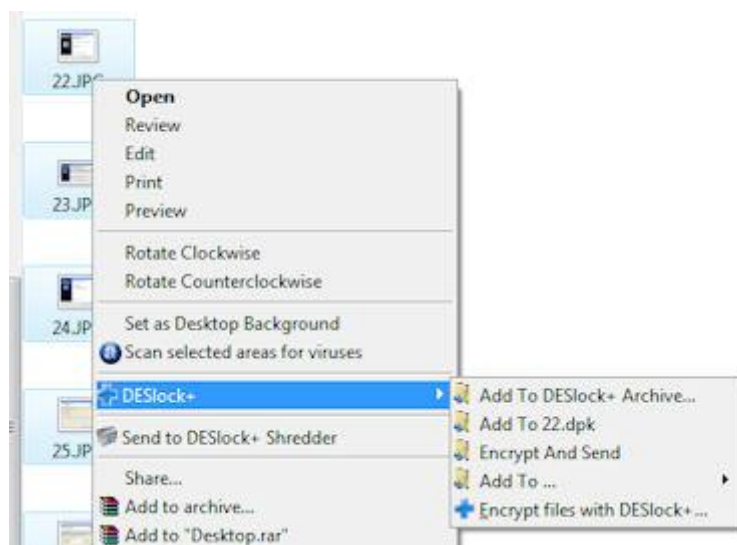
DESlock+ will then create an encrypted copy of the file, and leave the original exactly as it was. You can choose if you want to delete the (unencrypted) plain copy of the file when the process finishes. The encrypted file will appear as the example below, 'Secrets.txt.dlp'



For more information see the [File Encryption](#) section of the main manual.

Encrypted Archives - Quick Guide

Archives are used to create compressed, encrypted, versions of files, groups of files or folders to save disk space. To create an Archive, select a file, or a group of files, right click, then select DESlock+, then Add to DESlock+ Archive. You will then be prompted for an archive name and save location.



Then you need to specify an Encryption key to be used for the archive. Select a Key, press 'OK' and the archive will be created.



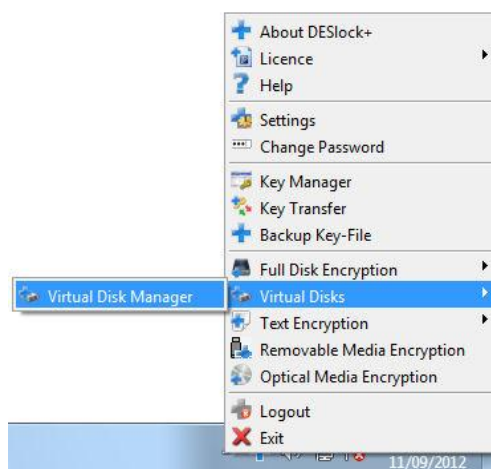
Double click on the Archive Icon and it will open in a new window. Then any further files you add will be encrypted and compressed and files removed will be decrypted and expanded. If you double click on any file within an Archive it will open and function as normal.

Note. If a DESlock+ Archive already exists in the current folder an extra option will appear on the DESlock+ right click menu, 'Add to...'. If the small arrow is expanded all available archives in that folder will be displayed.

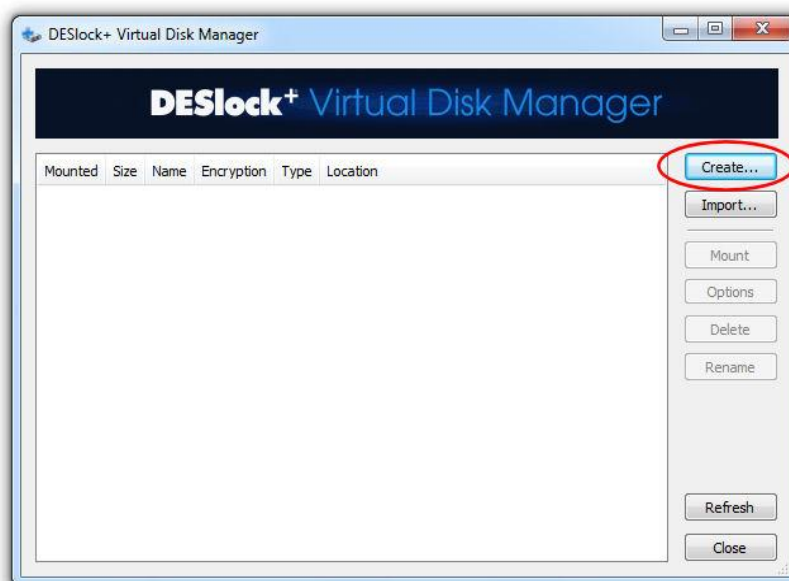
For more information see the [DESlock+ Archive](#) section of the main manual.

Virtual Disks - Quick Guide

To create a virtual disk, right click on the system tray icon (blue cross) and select 'Virtual Disks', then 'Virtual Disk Manager'.



Click on Create in the Virtual disk manager window.



In the next few windows provide the filename, and location and size of the drive you wish to create. Also decide if you want to use an encryption key or a password for the encryption. Next, select the key required or define the password.

Next, you will define the drive letter and mount / unmount options (whether the drive automatically starts and stops as you log into and out of DESlock+, or if you have to manually mount it yourself). Once all the parameters have been defined DESlock+ will create and format the new virtual disk. Once completed you need to mount the file (right click system tray, select 'Virtual Disk Manager', then 'Mount') before it can be used.

Once mounted, you can use the Disk as a normal drive attached to your computer: files added will be encrypted, files removed will be decrypted. Double click a file to open it with its normal application.

For more information see the [Virtual Disk Manager](#) section of the main manual.

Managed and Unmanaged users

DESlock+ user types

Managed User. A Managed User is one who is under the full control of an Administrator. The Administrator defines which DESlock+ functions the user has access to and can impose a wide range of operational policy onto that user. Managed users are controlled through the Enterprise Server and licensed through Vouchers, purchased by the Administrator, which are then supplied to the user. For more details of Managed Users and the Enterprise Server please refer to the Enterprise Server Manual or contact DESlock Ltd.

Managed users may not have access to all the features and functions of DESlock+. Managed users will have program and policy updates supplied by their Administrator, and cannot update from the DESlock+ website.

Unmanaged User. An Unmanaged or Stand alone user has full control of all their options, features and usages of DESlock+. Licences for standalone users are purchased direct from DESlock Ltd and registered to their own email addresses. Standalone licences may also be purchased by an Administrator using the Voucher system, and either supplied direct to the user from the DESlock+ website (User managed Licence), or supplied to the user by the administrator (administrator managed licence).

What am I?

A user can identify if theirs is a Managed installation with the appearance of the Enterprise Server Icon in their system tray, as examples below.



Installing DESlock+

Unmanaged (stand alone) users

If you are installing DESlock+ for a single machine operating without the DESlock+ Enterprise Server software, please follow the instructions in the [Quick Start Guide](#) or for detailed instructions on installing please see the section titled [Downloading and Installing](#)

Managed users

If you are working in a managed environment you will have been provided with an MSI installation package and an activation code by your systems administrator, either as a file or on a CD. This package contains specific policy settings for you as a user and for your workstation. Managed users should refer to their systems administrator for updates if required. Software or activation codes downloaded from the DESlock+ Website will not install or function over a managed installation.

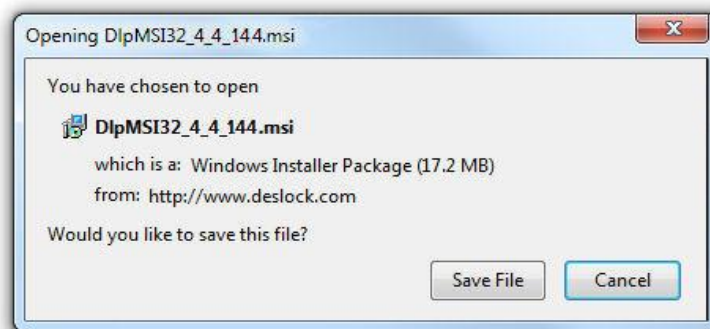
Downloading and Installing

If you are working in a managed environment you will have been provided with an MSI installation package and an activation code by your systems administrator, either as a file or on a CD. This package contains specific policy settings for you as a user and for your workstation. Managed users should refer to their systems administrator for updates if required. Software or activation codes downloaded from the DESlock+ Website will not install or function over a managed installation.

1. After registering at the DESlock+ Website you will be able to access the download page. Click on the green arrow in the right hand panel to download the software. Download the correct type for your Operating System (32 or 64 bit)

The screenshot shows two side-by-side panels from the DESlock+ website. The left panel, titled 'Your Licence', displays registration details: Registered to: sample@email.com, Type: Personal Edition, Registered Date: 22 Sep 2012, and Duration: Full Licence. Below this is a 'Your Activation Code' section with a blue button labeled 'NNNNN - NNNNN - NNNNN - NNNNN - NNNNN'. A note states: 'You will be asked for this activation code during installation.' There are also fields for a 30 character promo code and a 10 character code, each with a 'USE' button. The right panel, titled 'Your Downloads', shows 'Download DESlock+' with two download links: '32-bit DOWNLOAD' and '64-bit DOWNLOAD', both for version 4.4.144. Below these are 'Minimum System Requirements' listed for Windows 7, Vista, XP, and Server 2008/2003, along with hardware specs like Pentium 300MHz, 128MB RAM, and 64MB hard-disk space. A 'Release notes' link is also present.

2. File download Security Warning. Note; some of the following windows may display slightly differently depending on your operating system. Click 'Save' to save the file.



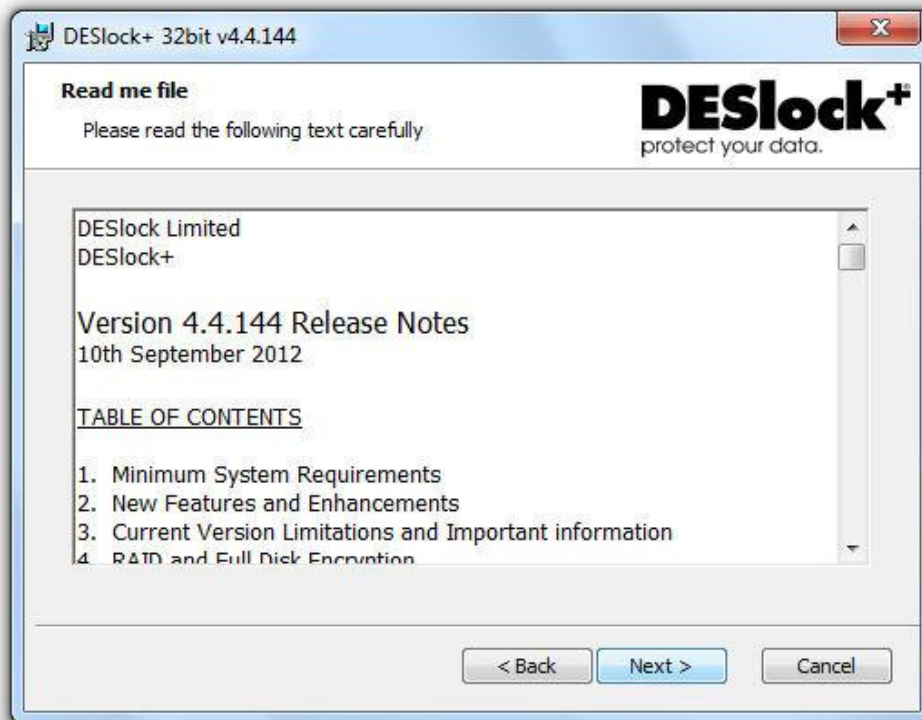
3. Save the file to a suitable location; do not change the file name.
4. Download Complete: When the download is complete, open the download location. You may have a 'downloaded files' window open, use right click to open the folder location for the downloaded file. Alternatively, depending on your browser, you may have to navigate to the download location.
5. Once the file opens the DESlock+ installation will start. Click 'Next'.



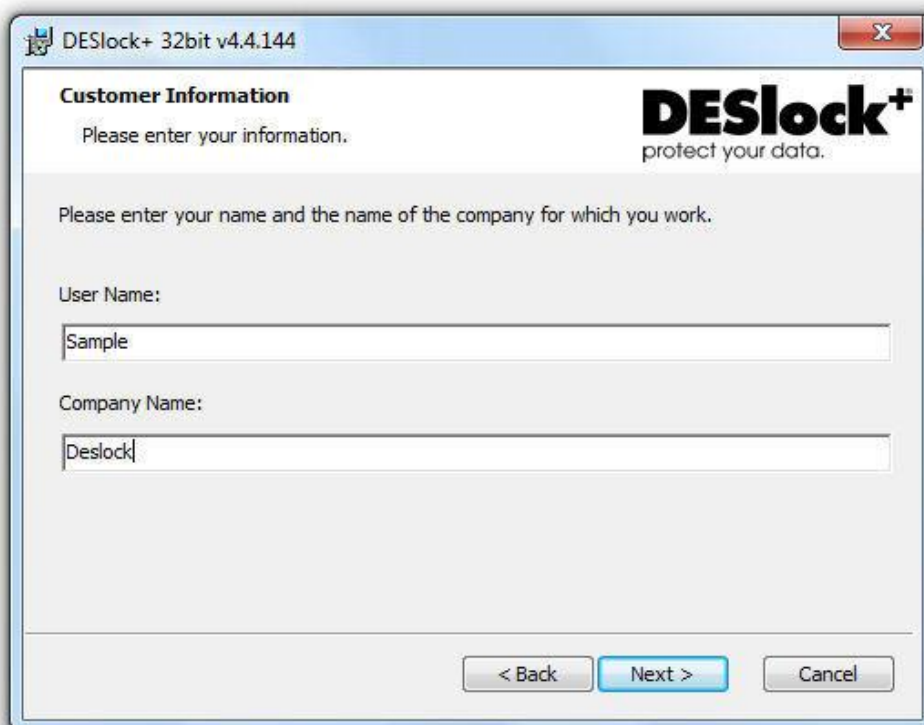
6. Read the End User License Agreement, ensure the 'I Accept' option is selected, and click 'Next'.



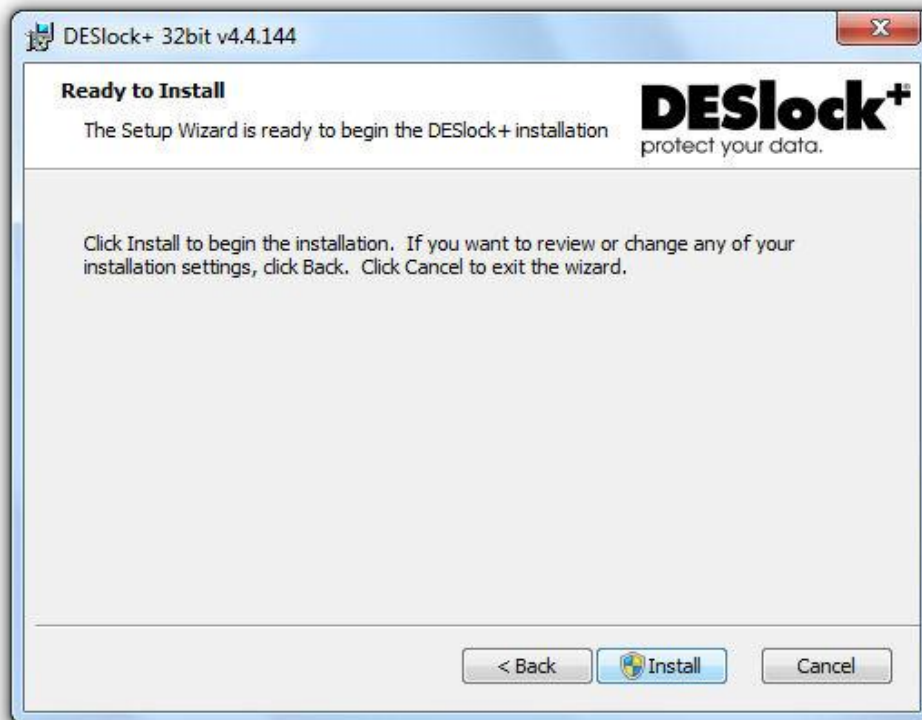
7. You then will then have the option to view the 'Read Me' file - this lists the latest changes and updates to the software, and highlights any known issues. Once you have read this, click 'Next'.



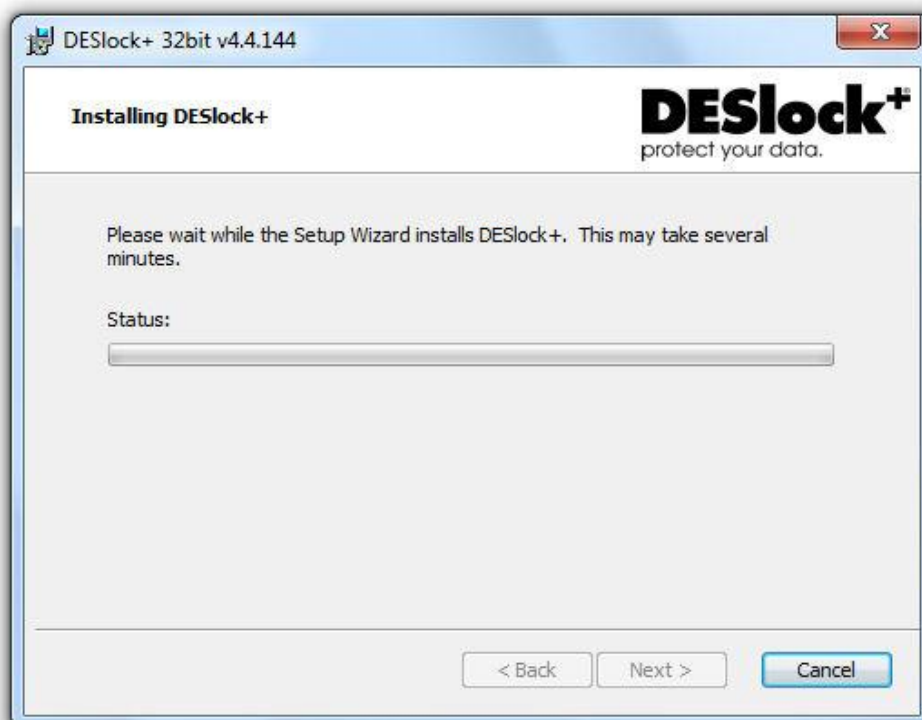
8. Enter your name and company details, then click 'Next'



9. Click 'Install' to install the software, or back to change any of the settings selected in the previous few steps.



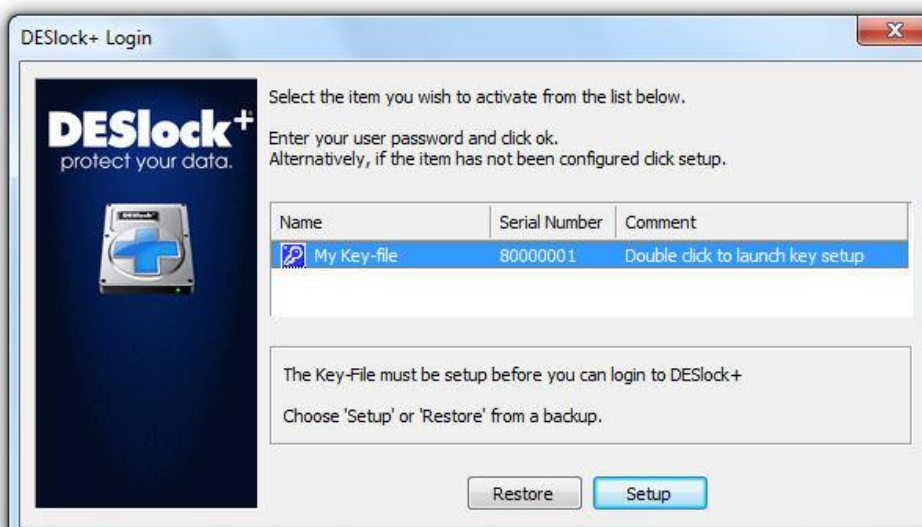
10. DESlock+ will then be installed.



11. To complete the installation you will need to restart your computer - So, save any work in progress, close any open programs and click 'Finish' to restart.



12. Once your computer has restarted, you will see the DESlock+ Login window, below. Select 'Setup' then refer to the [quick start guide](#) for the Setup process.



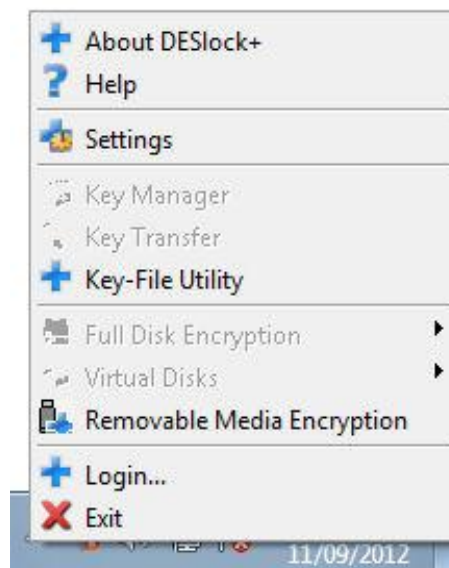
Login to DESlock+

Before use, DESlock+ will be in a disabled state, denoted by the disabled state icon in the system tray (See below). If you are a Windows 7 user, the Icon may be hidden. For more details see [Windows 7 System tray](#)



DESlock+ System Tray Icon.

To use DESlock+ you must login to a suitable configured Key-File. To do this, right click the DESlock+ icon (grey cross in system tray) and select **Login** (See Below).



DESlock+ Login.

The **DESlock+ Login** box will now be displayed (See below). Select the Key-File you wish to activate and enter the correct password for that Key-File and click OK. Press the Esc key to close the login box without logging in.



DESlock+ login box.

If the password was entered correctly, the DESlock+ icon in the system tray will change to the enabled state (blue cross, see below) and DESlock+ can now be used.



DESlock+ Icon enabled State.

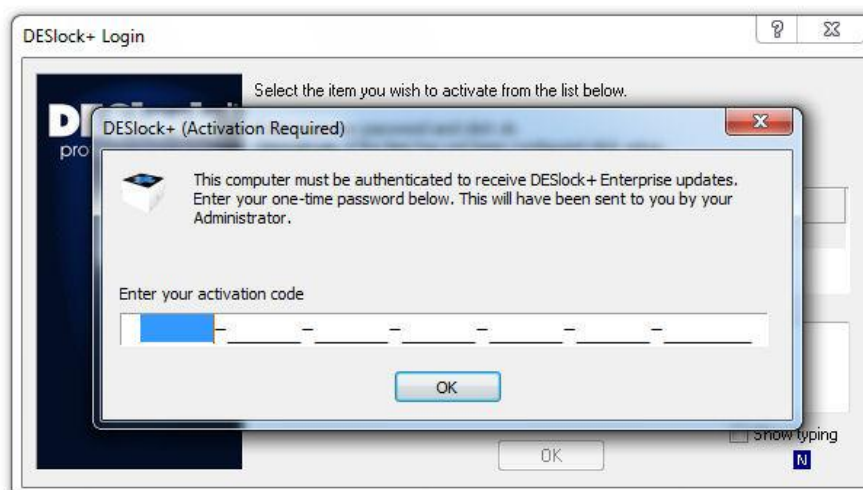
If the password was entered incorrectly, the user can attempt to login again. If an incorrect password is entered 5 times the Key-file will be disabled. Once disabled, further login attempts can only be made after the System has been rebooted. The number of attempts allowed cannot be changed.

If the login box instead prompts you to run the Setup Wizard then this must be used to configure the Key-File before first use. See the [Quick Start Guide](#) for details.

Login to DESlock+ - Managed Users

This section applies to users who are working in a managed environment, where the DESlock+ Enterprise Server software is used by a central administrator to control encryption policy across a workgroup or enterprise. If you are a standalone user please see [Login to DESlock+](#)

If this is the first time you have used DESlock+, once the software has been installed you will see the following window requesting an activation code. This code will have been provided to you by the administrator of the DESlock+ system within your organization.

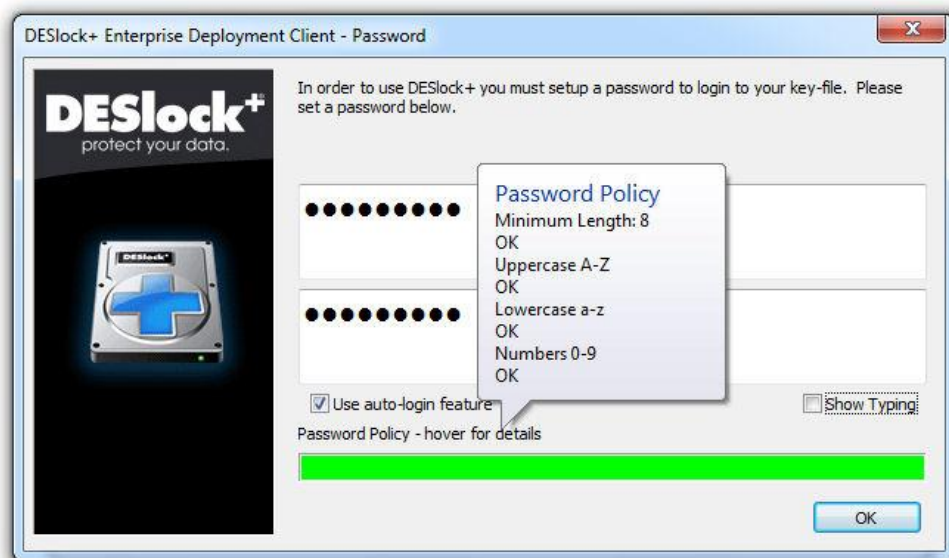


Once you have entered a valid code you will then be asked to create a user password. This is the password you will use to login to DESlock+.

The system administrator has the ability to enforce a password policy, for example, passwords to be a minimum number of characters and contain upper and / or lowercase letters and numbers. Whilst you type in your chosen password the password policy set will be displayed.



Once your password has been entered in both boxes and it conforms to the password policy the progress bar will change to green. Click 'OK' to continue.



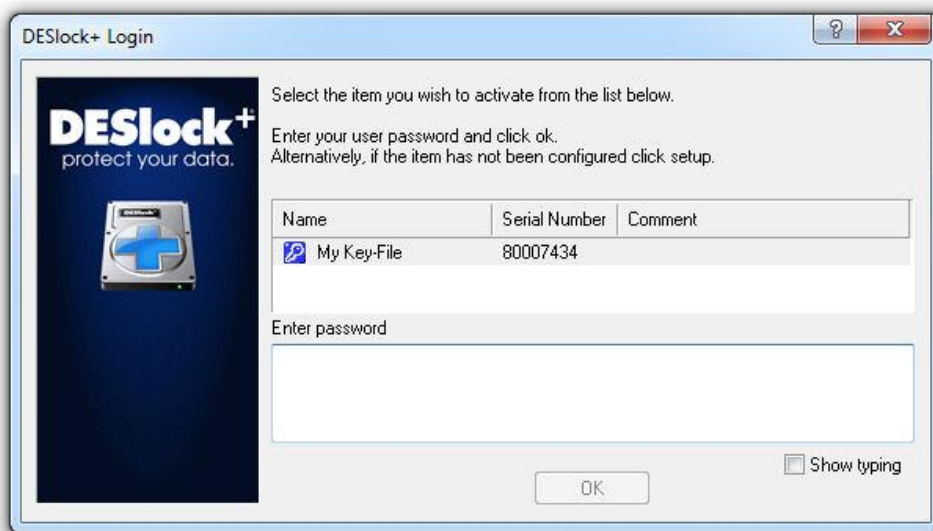
A message box will now appear briefly above the system tray to confirm that the system has been updated and has communicated successfully with the Enterprise Server software. Windows 7 users may find that these icons are hidden. See [Windows 7 System tray](#) for details on how to control the visibility of system tray icons.



Once you have logged into DESlock+ you will be able to access the DESlock+ features menu by right clicking on the DESlock+ (blue cross) icon in your system tray.



The next time you login to DESlock+ you will only need to enter your chosen user password and enter it in the login box (see below).



If the password was entered correctly, the DESlock+ icon in the system tray will change to the enabled state (blue cross, see below) and DESlock+ can now be used.

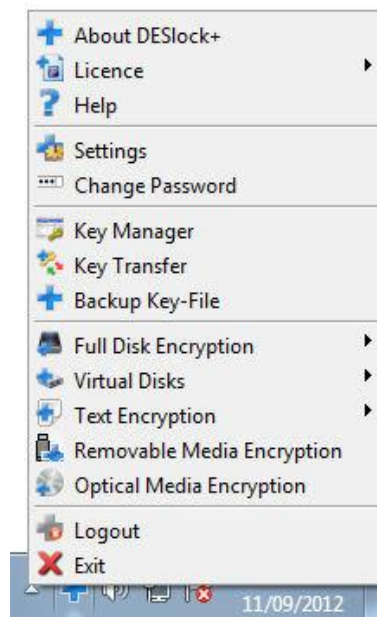


DESlock+ Icon enabled State.

System Tray menu

When DESlock+ is active, the system tray menu will change as shown below. Note that previously disabled menu items are now available and the **Login** entry has changed to **Logout**. To access this menu, right click on the DESlock+ tray Icon. If the Icon is not visible and you are a windows 7 user, please refer to this [section](#).

The feature set available is dependent on the type of licence you hold, in the example below the all features are available.



Active System Tray Menu

About DESlock+

The About Box will display product information such as Software Version, Licence type etc.



DESlock+ About Box.

[Licence](#)

Allows access to the Licence wizard, providing a simple means of upgrading your DESlock+ Licence.

[Help](#)

Displays help and documentation. (This Document)

[Settings](#)

This will launch the DESlock+ Settings Panel. This Panel is used to define how DESlock+ operates on your computer.

[Change Password](#)

Launches the Password Change Window - enter your existing Password and the new Password (twice) to change the Password.

[Key Manager](#)

The Encryption Key Manager dialog allows the user to create, delete and manage encryption keys.

[Key Transfer](#)

The Key Transfer Wizard allows encryption keys to be transferred between users.

[Backup Key-File](#)

Backup Key-File provides a simple Key-File backup system.

[Full Disk Encryption](#)

If not licenced for Full Disk Encryption, this will be greyed out and not accessible. If accessible this will start the DESlock+ Full Disk Encryption application. Note, before full disk encryption is initiated, further windows will appear, where the user specifies passwords etc to start Full Disk Encryption.

[Virtual Disks](#)

This will launch the DESlock+ Virtual Disk Manager, used to create encrypted Virtual Disks.

[Text Encryption](#)

This will launch DESlock+ Text Encryption, which can be used to encrypt Text directly, and the through the interface window (Settings) you can also define Hot Key combinations for many common actions to simplify the process.

[Removable Media Encryption.](#)

Starts the Removable Media Encryption Window, where you can Encrypt or Decrypt attached external drives.

[Optical Media Encryption.](#)

Starts the Optical Media Wizard, used to encrypt Optical Media. This includes CD's, DVD's, and Blue ray devices.

[Logout](#)

Clicking Logout will Log you out of DESlock+. To Log back in select Login from the Right click Tray Menu.

[Exit](#)

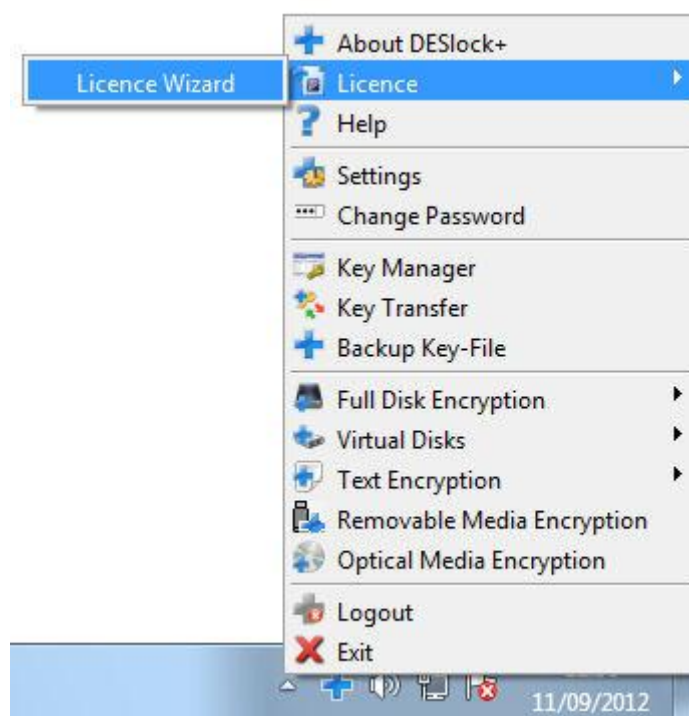
Clicking Exit will disable and close DESlock+. This will unload DESlock+ and remove the Icon from the system tray.

Licence Upgrade

The Licence Wizard is used to upgrade your copy of DESlock+ .

For example if you were upgrading from a free personal copy to DESlock+ Standard or Pro

- Go to the DESlock+ website.
- Click 'Products' then "Buy Now". This will provide you with a list of approved resellers.
- Alternatively you can buy directly from the DESlock+ website.
- To buy direct from DESlock+, Log in using your Website username and password.
- You will then see your existing activation code. Click 'buy Online' above the Licence window.
- Select and Purchase the required upgrade.
- Right click the DESlock+ icon in your system tray.



- Select licence at the top of the tray menu.
- Select Licence Wizard.
- Follow the Wizard to upgrade your version, adding the purchased features.
- Start using the new features.

Uninstall

IMPORTANT

Once DESlock+ has been uninstalled you will be unable to access any form of data that has been encrypted with DESlock+. DESlock Ltd will **not** be able to recover this data for you. It is your responsibility to ensure that all previously encrypted data has been decrypted.

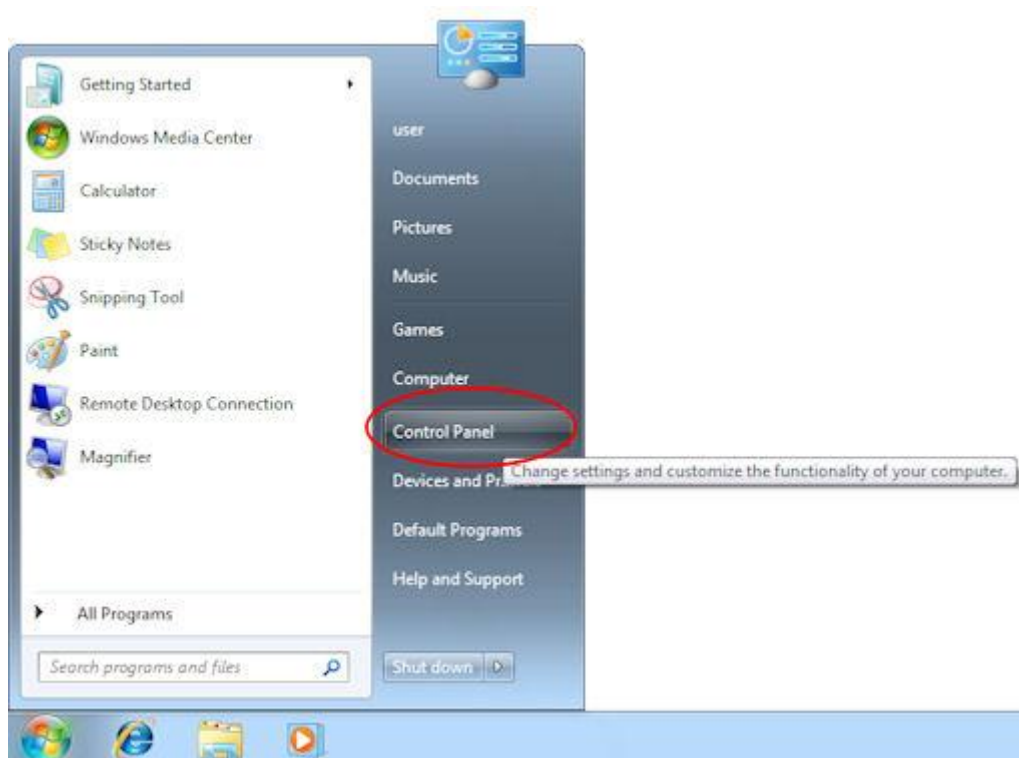
Before you uninstall DESlock+ make sure you:

- Decrypt any data, folders, files, text and archives that have been encrypted with DESlock+
- Decrypt any Hard drives or removable drives that have been encrypted with DESlock+
- Decrypt any backups that have been encrypted with DESlock+
- Decrypt any Mail that has been encrypted with DESlock+

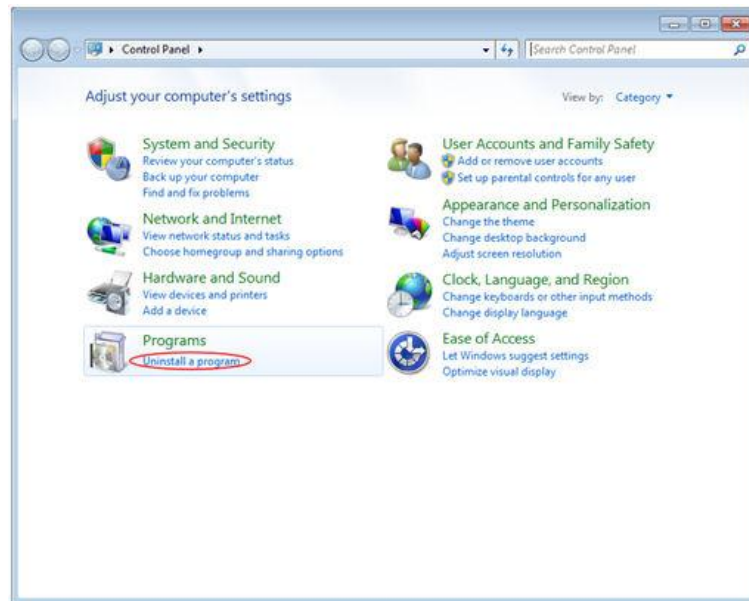
Notes

- if you have shared encryption keys with other users they will still be able to decrypt data encrypted with those shared keys, as long as they have access to it.
- Screen shots and process shown is for Windows 7, with other windows versions the process may differ slightly.

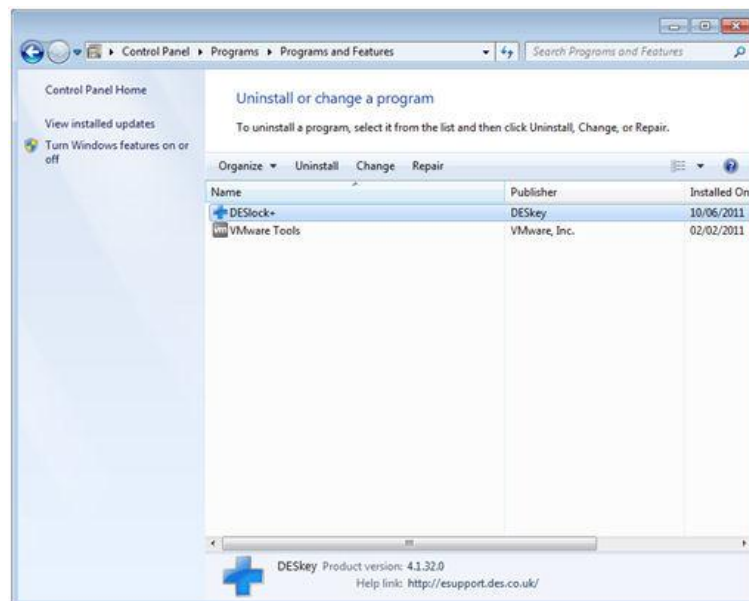
To uninstall DESlock+, click start, then select control panel.



In the control panel click on the link to 'uninstall a program' underneath the 'Programs' section. Note this window may appear in a different format, depending on your selected view. This example is shown in category view (top right hand of the window)



Windows will display a list of installed programs, highlight the DESlock+ entry and click Uninstall.



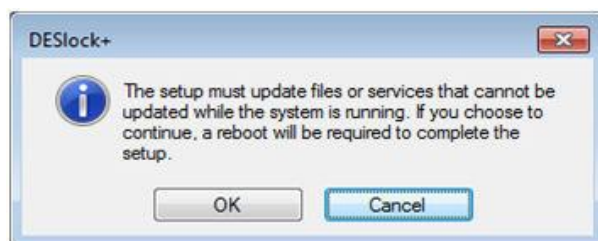
Select 'Yes', from the following window if you are sure you want to proceed.



Windows will start the un-installation process



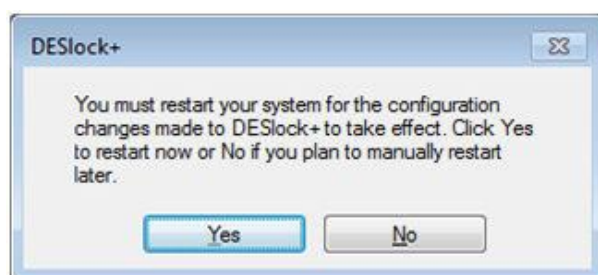
You will receive a warning that a Reboot will be required to complete the un-installation.



The uninstall wizard will then remove the program, with a status bar showing the progress. Depending on your system setup, you may have to accept a User Account control Warning before removal will be permitted. Click yes.



A restart will be required at the end of the process. This can take place automatically (make sure you have saved work and exited all other programs), or manually later. The un-installation will not be complete until after the restart has been performed.



Once the restart has completed DESlock+ will have been removed from your computer.

DESlock+ Settings

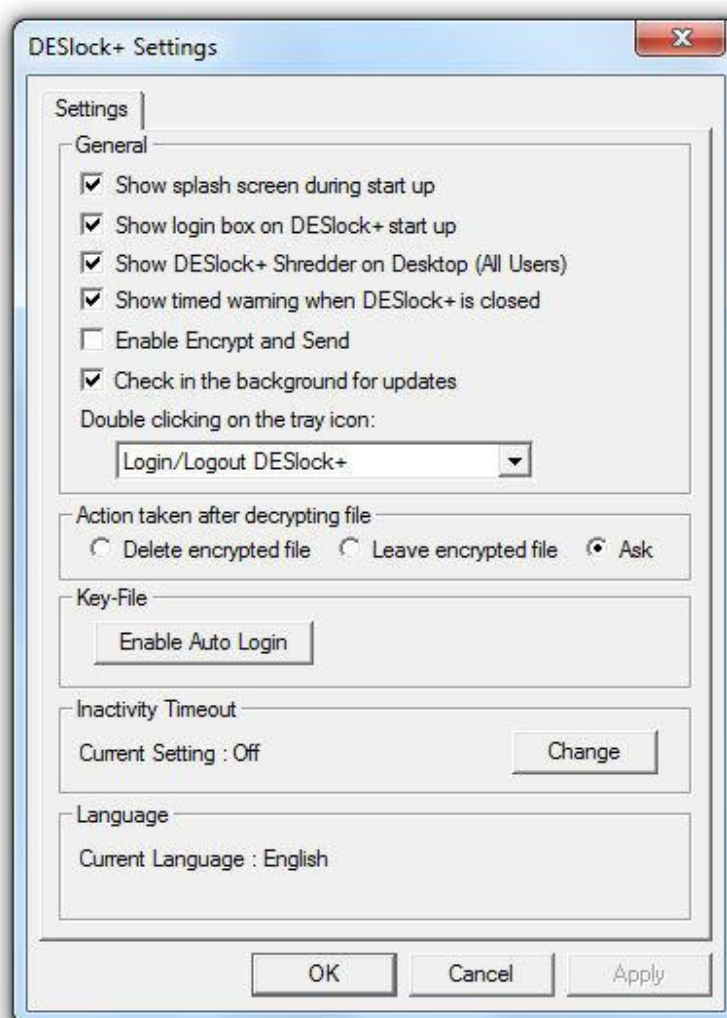
The DESlock+ Settings Panel allows the user to configure DESlock+ and to set various options. It can be launched by right clicking on the DESlock+ icon in the system tray and Selecting the Settings option. Some Settings options are dependent on the activated and licencing status of DESlock+ and may not be available at all times.

Note, with Windows 7 the system tray may need to be expanded to locate the DESlock+ Icon.

Depending on the type of software licence you have, some features of DESlock+ may not be accessible and the related options will therefore not be available in the Settings panel.

Note. If you are working in a managed environment the policy settings for you (as a user and for your workstation) will be set by the administrator of your DESlock+ system, and therefore some DESlock+ Settings may be unavailable.

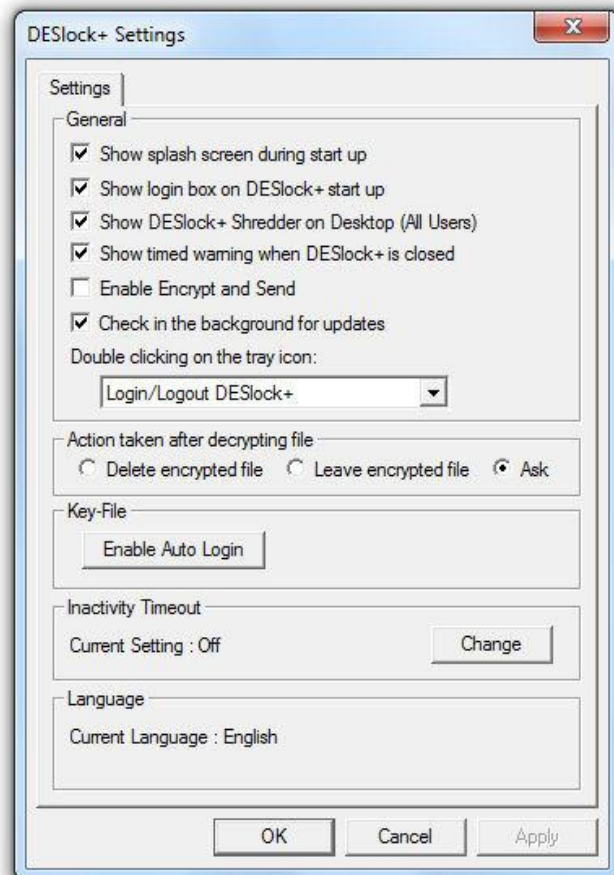
Typical DESlock+ Settings Panel



Settings

The Settings Window allows the DESlock+ options to be modified.

Note. If you are working in a managed environment the policy settings for you (as a user and for your workstation) will be set by the administrator of your DESlock+ system, and therefore some DESlock+ Settings may be unavailable.



DESlock+ Settings

General settings

Show splash screen during start up

Select to show the DESlock+ splash screen when the software starts.

Show login box on DESlock+ start up.

Select to show the user login box at Start up.

Show DESlock+ Shredder on Desktop (all users)

Select this to show the DESlock+ Shredder icon on the desktop. This will affect all users.

Show timed warning when DESlock+ is closed

If this option is selected, a warning box (below) will be displayed if the user attempts to **exit** the application. The shutdown can be cancelled before the 10 second timeout completes.



DESlock+ exit warning

Enable Encrypt and Send

If selected, the DESlock+ sub menu (right click on a file) will allow a file to be encrypted and sent via mail as an archive or as an encrypted file.

Check in the background for updates

If selected, DESlock+ will periodically check for updates via the internet. If a new update is available the user will be advised and given the option of installing or not.

Double click Tray Icon settings.

Defines the action that will be performed when double clicking the tray Icon. (Login/Logout DESlock+, Launch the Settings panel, Key Manager, Key Transfer Wizard, or the Virtual Disk Manager)

Action taken after decrypting file.

Defines the action taken after decrypting an encrypted file;

The options are:

- Delete Encrypted file - encrypted file is deleted, leaving the decrypted version available.
- Leave Encrypted file - both the plain and encrypted versions of the file are left.
- Ask - the program requests the action to be taken in each case.

Key File

Auto login - The user will be automatically logged into DESlock+ at the windows login. There will be no separate DESlock+ login when the system is started, however, if the user logs out of DESlock+, the login window will be displayed if the user right clicks on the DESlock+ icon in the system tray.

Inactivity Timeout Settings

Defines the inactivity settings for DESlock+, after which DESlock+ may log out automatically. These may be:

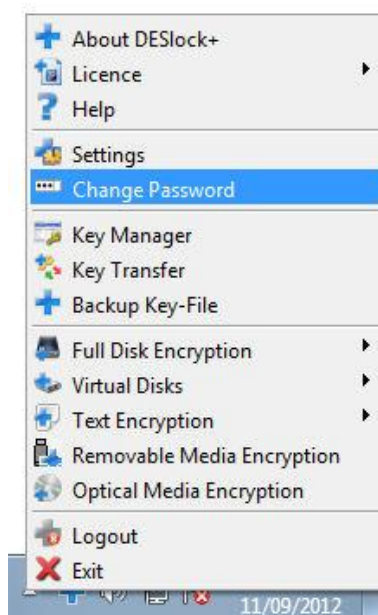
- Do Not Disable - DESlock+ remain logged in regardless of inactivity.
- Use Windows screensaver - DESlock+ is logged out when the Windows screensaver is activated. Note, the windows screen saver has to be enabled for this option to be available.
- User inactivity - After a user defined period of inactivity DESlock+ will log out.

Language

Shows the current language setting of DESlock+.

Changing Password

To change the password, click the 'Change Password' option on the system tray menu, and then enter the old and new passwords - see below.



Enter the old password, then the new one, twice. Click OK to accept the changes.

You can also tick the 'Auto logon' box. The user will be automatically logged into DESlock+ at the windows login. There will be no separate DESlock+ login when the system is started, however, if the user logs out of DESlock+, the login window will be displayed if the user right clicks on the DESlock+ icon in the system tray.

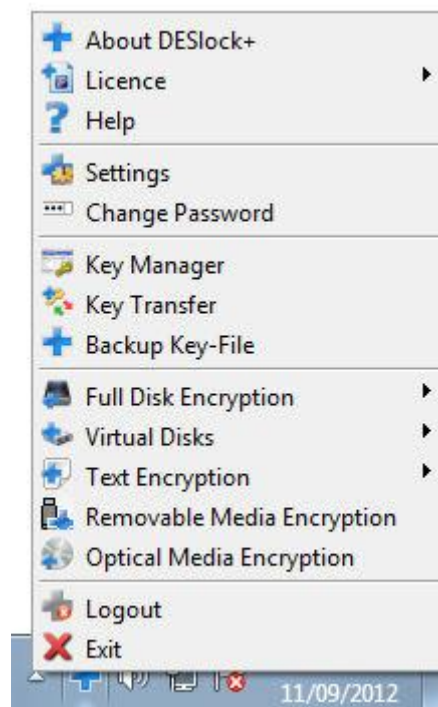


Encryption Keys

Encryption keys are allocated key slots within a Key-File. DESlock+ can provide up to 64 key slots depending on the type of licence that was used to create the Key-File.

Each slot may contain an encryption key, and each encryption key must be unique. The ability to store multiple encryption keys means different encryption keys may be shared between different users, allowing data to be securely exchanged between different members of a group without any one member necessarily being able to access all of the data.

Encryption Key administration can be performed via the Key Manager, Key Transfer and Backup key-file headings which can be accessed from the DESlock+ System Tray menu.



Key Manager

The Encryption Key Manager allows encryption keys to be created, renamed, deleted and the Key file itself to be renamed. It displays a list of the available key slots within the active Key-File and will allow various operations on the encryption keys or the empty slots. Key backups are performed using a separate utility.



Encryption Key Manager






Key Storage Space

The Key Manager display is split into 5 columns for each key slot available. These columns are as follows:

Key Slot

The location of the encryption key in the Key-file storage space.

The following icons can be displayed alongside the slot number:

Icon	Meaning
	The slot contains the default encryption key. Note the text will also be bold.
	The slot contains an encryption key but it is not set as the default key.
	The slot does not currently contain an encryption key.
 	The slot contains an encryption key (which may be the default encryption key) but there is no record that a backup file or database entry has been made. If this encryption key is lost then data encrypted using this key may be unrecoverable.

Name

A user definable descriptive name given to the encryption key. For example this could be the name of a person, a department or a project.

Type

The name of the algorithm the key can be used with. The various algorithm types available are AES (Rijndael), 3DES (Triple DES) and Blowfish. These are described in detail in [Technical Information](#).



Length

The length of the key measured in bits. AES and Blowfish keys are 128-bits long. The 3DES key is 112-bits and comprises 2 unique 56-bit DES keys. Key length cannot be changed for these algorithms.

Terminator Code

The current value of the Terminator Code. Use of the terminator code is described in detail in the [Terminator and Group Code Section](#).

The following icons are displayed to represent terminator code status.

Icon	Meaning
 5	The Terminator Code value of this key is set to 5. This key can be transferred with a new Terminator Code value less than the value displayed i.e. the value can be no greater than 4.
 0	The Terminator Code value of this key is zero. This key cannot be transferred under any circumstances.

The default terminator value for new keys is 255.

When issuing an encryption key, the Terminator Code of the original key will not change. The new value specifies the Terminator Code value of the encryption key within the destination Key-file.

Encryption Key Options

The following options are available on an empty key slot:

Generate

This will allow new encryption keys to be created and stored within the Key-File. A wizard (See [Key Generation Wizard](#)) will guide the user through this process.

The following options are available on a highlighted encryption key:

Delete

This will remove an encryption key from the Key-file key space.

Rename

This will rename an encryption key in the Key-file key space.

Make Default

This makes an encryption key the default encryption key, which means it will always be initially selected in the key choosing dialog when an encryption process occurs.

Renaming a Key File.

The key file can be renamed through the Key Manager by double clicking the key file name at the

top of the key manager and entering the new name.



Key Generation Wizard

The Key Generation Wizard is used to create new encryption keys. New keys can be used to encrypt data and can also be transferred to other Key-Files if desired.

Generating a new Encryption Key

First, select an empty slot in the Key Manager then click on the 'Generate' button.

When the wizard is launched, the welcome screen is shown. Click **Next** to begin key generation.



Key Generation Wizard

Enter a name to identify the encryption key. This name can be anything for example the name of a person or the name of a project with which the key will be used.

The **Set as default key** checkbox is used to set this key as the default key for encryption. The default key will always be initially highlighted when selecting encryption keys. Click **Next** to continue.



Key Name

Select the type of encryption key to generate. This relates to the algorithm that the key will be

used with.

The different types of algorithm are described in more detail in [Technical Information](#). A brief description is also given in the Algorithm Details box. Click **Next**.



Encryption algorithm selection

The new key has now been generated and added to the Key-file key space. It can now be used for encryption of data. The terminator code value of all new keys will be 255. Click Finish to end the Wizard.



Key generation completion

Key File Backup.

Important. Any changes to the Key File (keys created, deleted, or the Key file password changed), will trigger the automatic Key File backup system to run. See [Quick Backup](#) for details.

Transferring Encryption Keys

Why the need for transfers

In order for two (or more) DESlock+ users to be able to access common encrypted data, their Key-Files must both contain the same encryption key. As two Key-Files cannot generate the same encryption key, an encryption key must be generated in one and then transferred to the other.

How transfers work

All encryption key transfers are secured by RSA encryption. Put simply, this is a recognised method of protecting the key being transferred so that only the receiving device can use it. In practice it means that the Key being transferred is encrypted by the receiving key-file's public encryption key. In this way the key being transferred is secure (the file is encrypted), and only the receiver can decrypt and use the file.

The fact that the transfer can only occur if the destination is explicitly specified (through the public key of the receiver) has important implications for encryption key backups, which are covered later.

Transfer stages

The process of transferring an encryption key can be thought of as four distinct steps.

- The Recipient gains access to data encrypted with a key they do not have (ie receives some files by email, FTP, CD etc)
- The Recipient generates a Key Request for the Originator of the data. This request extracts the public key from their Key-File in a form that can be sent to the Originator.
- The Originator creates an encryption Key Update using the supplied Key Request. This extract uses the supplied public key (the request) to protect (encrypt) the requested key to create an 'encryption key update'.
- The Recipient uses the update to add the encryption key into the key space of their Key-File.

Because the transfer processes uses the RSA algorithm, and because no two Key-Files will have the same public key "pair" a supplied encryption key update will only be useful to the intended recipient of the update.

Key Transfer Wizard

To effect encryption Key Transfers, DESlock+ provides the Key Transfer Wizard. This wizard simplifies the transfer process, allowing encryption keys to be easily transferred from one Key-File to another.

See the [Key Transfer Wizard](#) for more detail.

Key Transfer Wizard

The Key Transfer Wizard has three steps designed to allow encryption keys to be transferred between Key-Files.



Whenever an encryption key is required to decrypt data, but is not present within the active Key-file, it can be requested using this wizard. Please refer to the overview of the [Key Transfer Process](#), if you require additional clarification on the steps involved.

The three steps involved in key transfer are:

- Key Request
- Key Issue
- Key Update

The request and update steps are performed by the user requesting the key. The Issue step is performed by the user issuing the key.

Files used in the key transfer process will have one of the following two icons.

Icon	Meaning
	A DESlock+ Key Request file (file extension .DLR).
	A DESlock+ Key Update file (file extension .DLU).

As files created in the backup process are equivalent to DESlock+ Key Update files, the Key Transfer Wizard can also be used to add encryption key backups to a Key-file. The creation of backup files is described in 'Encryption Key Backup using the Key Manager' in [Encryption Key Backups](#).

Transferring Encryption Keys

When the Wizard is launched the option screen is shown.



Key Transfer Wizard

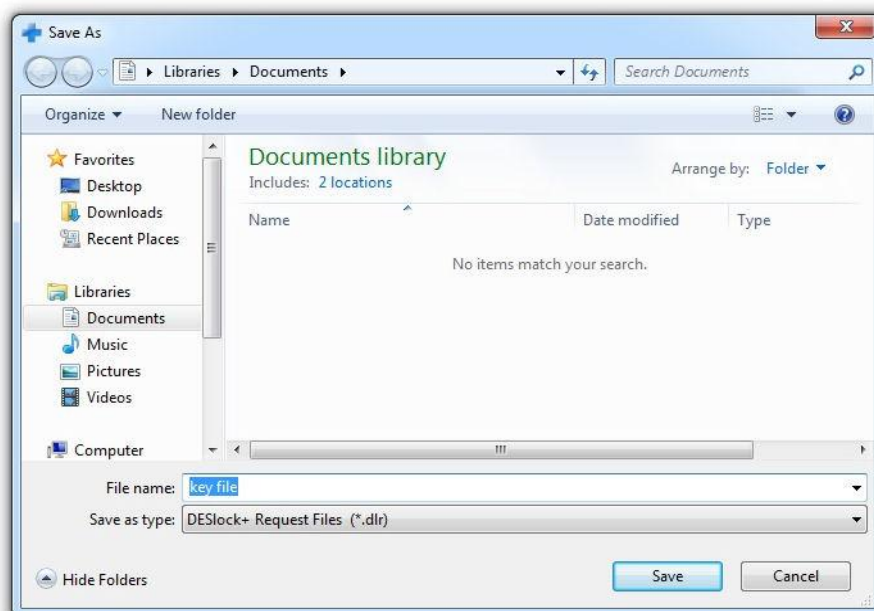
If the Wizard is launched by the Outlook plug-in, this screen is not shown as the desired action is already known.

Similarly if launched from the Key Transfer Database applet, or if double clicking on a .DLU or .DLR file, the Wizard will be launched with the appropriate option selected.

Request a key from another user

The request option of the Key Transfer Wizard will create a request file which contains the public key of that Key-File. This information is necessary to issue an encryption key.

Either 'browse' for or manually enter the location and filename to store the request. Click **Save**.



Key transfer request

The request is complete and the request file has been saved to the location specified. This file must now be sent to the issuing Key-File, for example by email.



Key Transfer file location

Issue a key to another user

The issue option of the Key Transfer Wizard will extract an Encryption Key and protect it with the Public Key of the requesting Key-File. A copy of the Public Key must be available either from details stored in the Key Transfer Database or by using a request file.

Either **Browse** for or manually enter the path and filename of the request file created by the requesting Key-file. Or alternatively, if it is listed, select the Key-File from the Key Transfer Database. Click **Next**.



Open Request file

Details of a Key-file will be stored in the Key Transfer Database if the requesting Key-File was setup using the Key-File Setup Wizard on the same computer, or the public key was chosen to be added to the database during a previous key transfer operation.

If a request file is used and the key details of the public key are not already stored in the local Key Transfer Database, the user will be given the option of adding the public key here.

Select the encryption key you wish to issue. Any of the keys can be issued provided the Terminator Code is non zero. When the desired key has been selected, click **Next**.



Key transfer key selection

Set the new value for the Terminator Code. The new value must be less than the Terminator Code of the encryption key in the issuing Key-file. For example, if the key being issued has a Terminator Code of 5 then the new value must be between 0 and 4 (inclusive). If a value is not explicitly set the default is zero. This value relates to the value assigned to the Terminator Code in the requesting Key-file and will not modify the original copy in the issuing Key-File.

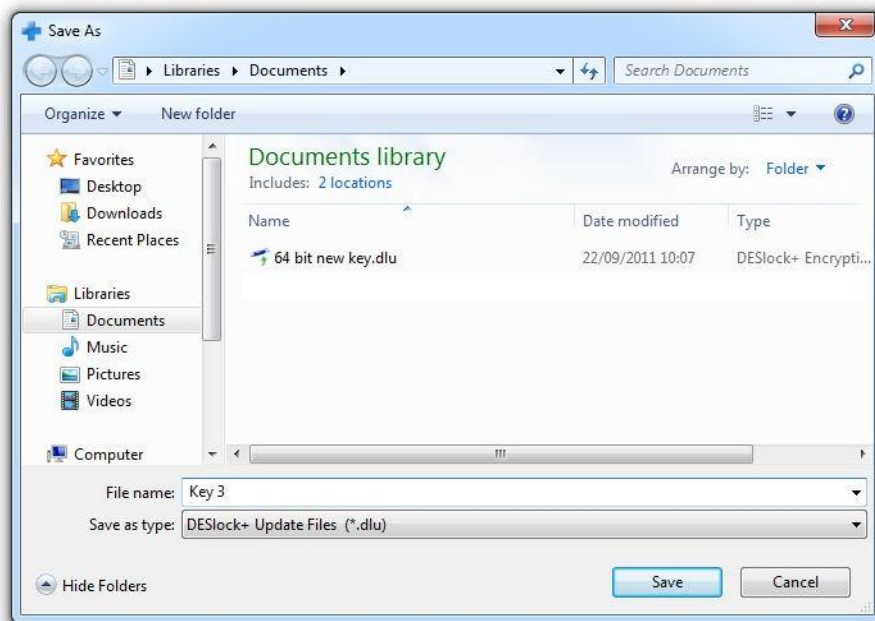
If 'Tie to group code' is selected, this restricts further transfer as the key must stay within the group. The option is only available if the current Key-File is a member of a group.



Key transfer Terminator Code

Either 'browse' for or manually enter the location and filename for the update file. This file will contain the selected encryption key, protected by the public key of the requesting Key-file so that the key can only be added to the requesting Key-file. This file will need to be used by the

requesting Key-file during the update procedure.



Key transfer update file



The Issue is complete and the update file has been saved to the location specified. This file must now be sent to the requesting Key-File.



Key transfer update file location

Update your DESlock+ Key File with a key from another user.

The update option of the Key Transfer Wizard will update your Key-file with an encryption key from another Key-File. This includes encryption keys sent by other users or encryption keys that have been backed up to a file.

Either **Browse** for or manually enter the path and filename of the update file. Click **Next**.



Key transfer updating key

Once the file has been opened, the location in the key storage space of the Key-File must be specified. The name of the encryption key and the Terminator Code will be displayed. Once a suitable location has been specified click 'Next'.



Key transfer key location

The update is complete and this Key-File now contains the new encryption key. Files can now be encrypted or decrypted using this key.



Key transfer completion

Note. Every time the DESlock+ Key File is changed, in this case keys added, the Key File backup routine automatically starts. In this way you will always have a backup of the current state of your key file, which should always be stored away from your Main hard drive for security and recovery purposes. You cannot cancel the key automatic backup system. For more details see the [Encryption Key Backups](#) section.

Encryption Key Backups

Why backups are important

Backing up an encryption key is important because if the only copy of a key is lost then there is no way to access data encrypted with that key. There are no backdoors in the software and you cannot generate the same encryption key again if it is lost. Therefore it is important the encryption key is never lost.

Backups are performed so the encryption key is stored in another Key-File or a Key File Backup. If one Key-File is lost, through damage or theft or other reasons, the encryption key can still be obtained from the other Key-File or Back up.

The Quick Backup process creates a complete copy of the Key-File, together with all the Encryption Keys in it.

Individual keys may be backed up using the Key Transfer process, with the key being held by another key file. In most situations the [Quick Backup](#) process should be used, but in environments with multiple Key-Files and complex Encryption Key structures it may be preferable to use the Transfer process.

Every time the DESlock+ Key File is changed, keys added, deleted or the password is altered, the Key File backup routine automatically starts. In this way you will always have a backup of the current state of your key file, which should always be stored away from your Main hard drive for security and recovery purposes.

See the [Quick Backup](#) process for more details, and the [Key Transfer Wizard](#) if this method is chosen.

Quick Backup

This simple and quick process will create a backup copy of your Key-File, with all encryption keys and settings included. It is recommended that you save this backup to a removable memory device, or in your normal data Backup location. In this way, if your hard disk crashes, when you restore your data from backup, your key is also available. To recover a Key-File Backup see [Key-File Utility](#)

1. Right click on the System tray menu and select Backup Key-File.

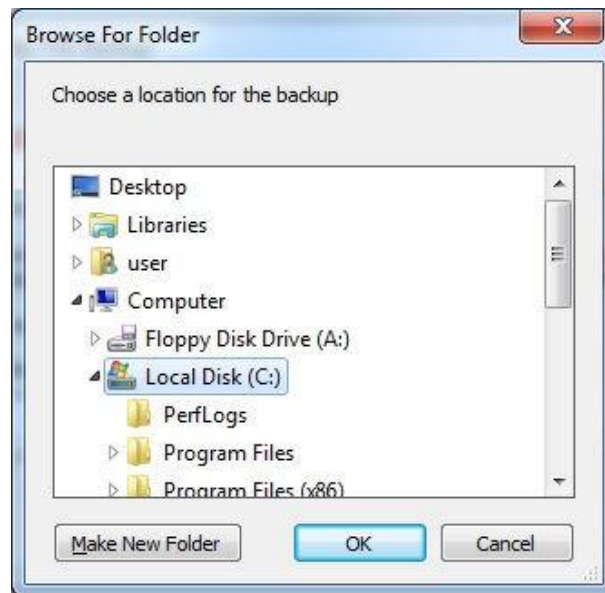


2. You will then see the message below. Click browse to select a backup file location.

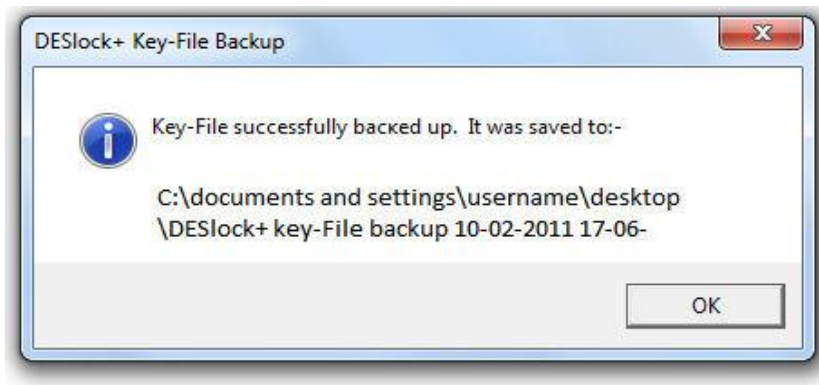


Note. Once you have defined a Backup location, if you select the 'Always use this folder in future and do not show this dialog' check box all future backups will be created silently, without any user intervention.

3. Select a suitable location for the Key-File Backup, and click 'OK'.



4. Your Backup will be created and a similar message to the one below will be displayed. The backup name includes the date and time.



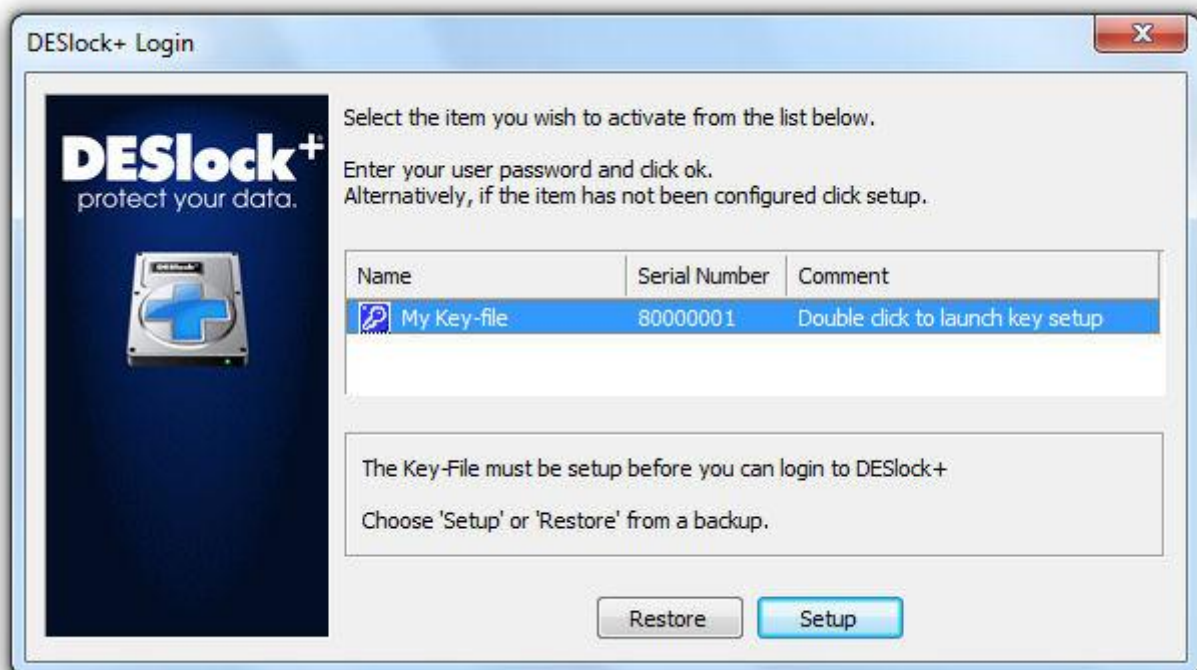
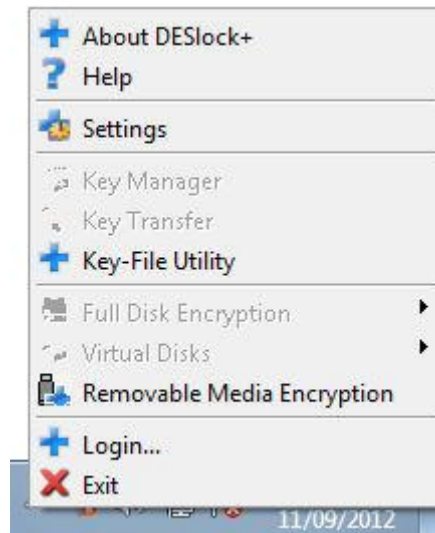
5. If you selected to save the Backup to your main hard drive you will see the warning message below, either select 'Yes' to continue or 'No' to re-specify a new backup location.



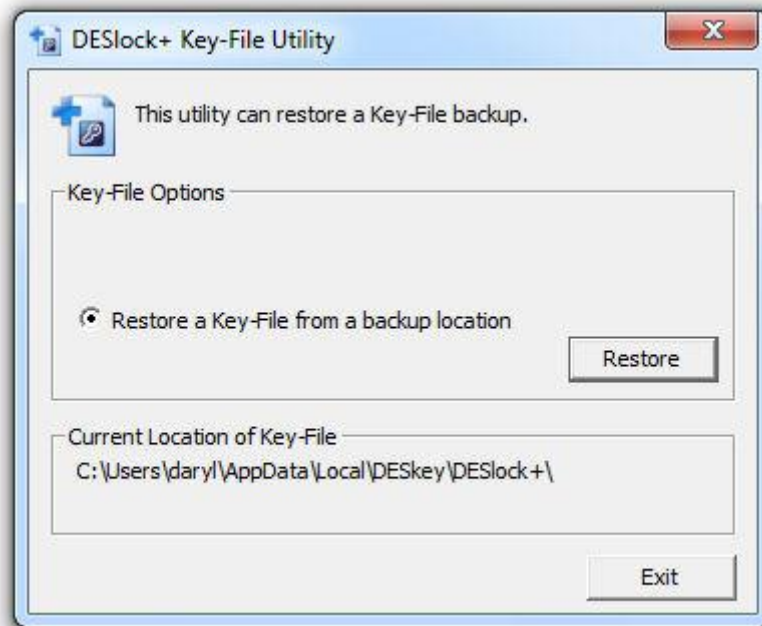
Key-File Restore Utility

The DESlock+ Key-File utility is used to restore a Key-File from a backup location. Each time a key file is changed the User is forced to take a Key-file backup for security. See [Encryption Key Backups](#) for more details.

To restore a backup the DESlock+ Key File utility is required. Note, not only can this be used to restore a backup, it can also be used to move your Key File between computers, for example on a Memory Stick. The Key File Utility can be started from the DESlock plus System tray icon while the user is **LOGGED OUT** of DESlock+. It may also be started from a new installation at the initial Login/Setup window.



The Key-File utility will display the current location of the Key-File, and allow you to restore it from a backup location. Note, the Backup location may be different from the Key-File location - this is defined by the user when the backup is made.



Key-file utility

Clicking Restore will allow you to navigate to the location where the Key File backup is stored. Select the folder containing the backup you wish to restore and click ok. If the location only contains one backup, that will be automatically used. If more than one backup file exists you will be prompted to select the backup to be restored.

Terminator and Group codes

Description

Terminator Codes. The terminator code is a setting in an encryption key used to limit authorised copying.

To transfer a key to another Key-File the terminator code value must be more than 0. If you set it to 1, anyone you provide the key to can copy the key on to other users (as many as they like), but those additional users will not be able to share the key with other users. When a key is transferred, the Terminator Code is decremented in the copy, but remains unchanged in the original. The greater the Terminator Code, the more "levels" it can be transferred to.

Group codes. Group codes are used to restrict encryption key transfers within corporate environments.

The Group Code defines a group the Key-File is a member of and can be used to restrict key transfers in addition to the terminator code. By default, a Key-File will not be a member of any group and any encryption keys generated can, assuming a valid terminator code, be transferred to any other Key-File. However, if the Key-file is a member of a group, encryption keys generated can be tied to the group so that they cannot be transferred outside the group. However, the Key-File will retain the ability to generate encryption keys that can be transferred outside the group if necessary.

A Key-File can be a member of only one group at any one time. The Group Code must be set by DESlock Ltd.

Terminator Code Example

In many cases when a common encryption key is transferred between users, the originator will want to decide whether or not a recipient can forward the key to another user.

Suppose User "A" creates a new project key and wishes to share it with others on the project team. User "A" sends the key to "B" and "C" with a Terminator Code of 0, to User "D" with a code of 1 and to User "E" with a code of 2.

Users "B" and "C" cannot copy the key any further.

User "D" can copy the key to other users, in this case "F" and "G".

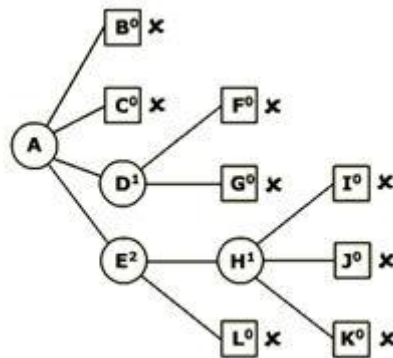
Because the Terminator Code is decremented at every generation, users "F" and "G" cannot copy the key.

User "E" had a value of 2, who copied the key to user "H" who in turn copied it to "I", "J" and "K".

"I", "J" and "K" cannot copy the key any further.

User "E" also copied it to User "L" but in this instance manually reduced the Terminator Code to 0 (it cannot be increased or kept constant.)

"L" is unable to copy the key any further.



Terminator code use

To retain full control of a key, always set the terminator code to Zero. In this way you will be able to provide the key to other users. They will not be able to forward the key onto anyone else.

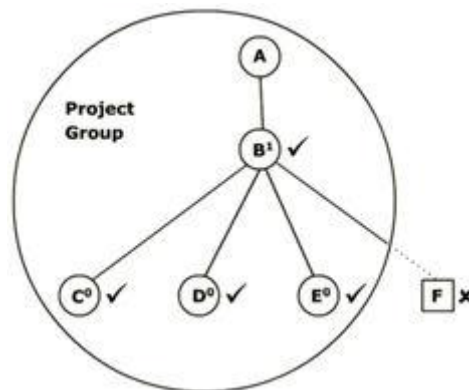
Group Code Example

To maintain data security, it is often necessary to control key transfers within a defined group.

In this example, user "A" creates a new project key and wishes to share it with others on the project team. Group Code has been assigned to match that of User "A's" Key-file.

User "A" has previously issued "B", "C", "D" and "E" with Key-files having the correct fixed Group Code. User "F" is not a project team member and does not have a correctly coded Key-file.

User "A" transfers the key to "B", with a terminator code of 1. "B" is then left to update the other users. "C", "D" and "E" are successfully updated, but "F" cannot receive the encryption key as they do not have the correct Group Code.



Terminator code example

Encrypting with DESlock+

There are many ways to encrypt data using DESlock+, click on the heading for more information:

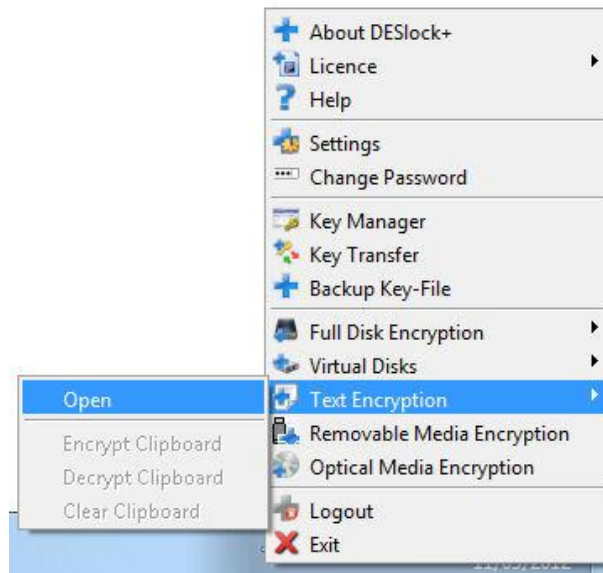
- [Text Encryption](#) - part or all of a document may be encrypted/decrypted manually, using DESlock+ Text Encryption tools.
- [File Encryption](#) - Individual files can be encrypted/decrypted manually. This allows, for example, a file to be securely sent via email or on a CD/removable media.
- [Folder Encryption](#) - An entire folder is encrypted. Any files in it and any placed in it at a later date are encrypted. Sub folders are also encrypted. As files are opened normally (by their applications) the process of decryption/encryption is transparent to the user.
- [Archive](#) - Encrypts and compresses all data placed within it.
- [Virtual Disks](#) - An encrypted file that can be mounted as a disk drive. All data on the Virtual disk will be encrypted, and can be accessed and used as a normal disk drive.
- [Removable Media](#) - Removable media (eg USB HDD, USB memory sticks) can be either fully encrypted or file mode encrypted.
- [Optical Media](#) - Optical Media (E.g. DVD/CD's) Your selected files are encrypted, then burnt to the optical media.
- [Full Disk](#) - Full Disk Encryption - FDE - your entire hard disk is encrypted - All files, folders and data, including all system files.

Note. Text and files encrypted with a password may be decrypted using the [DLP reader](#), and therefore accessible to users without DESlock+ installed.

Text Encryption

Text Encryption is a simple utility that allows the Encryption and Decryption of text within a window (Text files, word files, web browsers etc - any window with selectable text)

To access right click on the DESlock+ Icon in the System tray and select '**Text Encryption**' followed by '**Open**'.



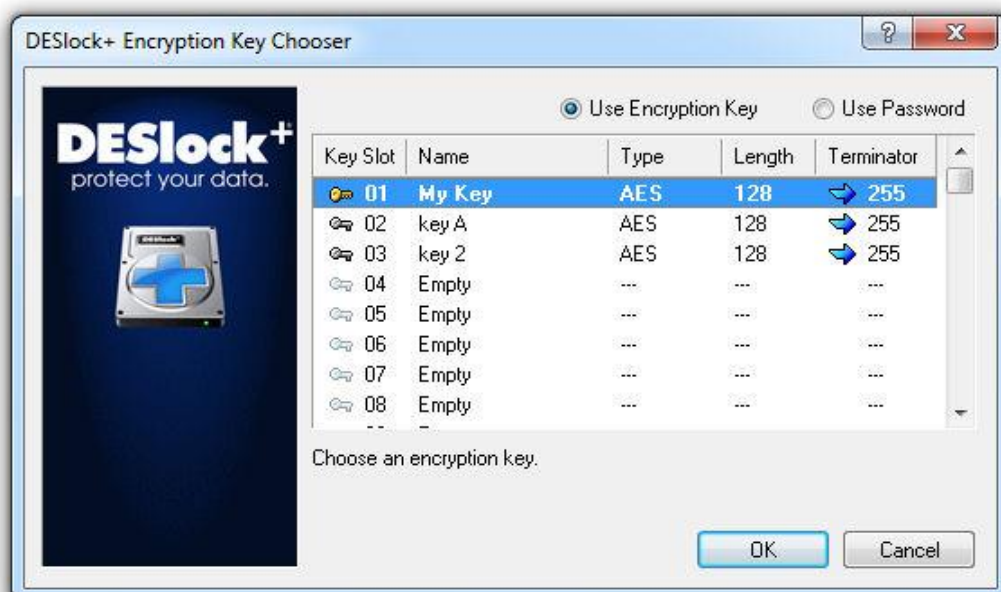
This opens the Text Encryption Dialog which allows the text in the current window (or selected text or the contents of the windows clipboard) to be encrypted/decrypted (and also decrypted to the viewer).



Encrypt Window

To use for the current (Last accessed) window, open the Text Encryption dialog from the system tray, click back into the window to be encrypted, then with the 'Encrypt Window' tab selected (as above), click the 'Encrypt' button. DESlock+ will auto select all the text in the window then prompt for an Encryption Key (or Password/phrase). The Text will be encrypted with that Key (or

Password) and auto pasted over the original Text.



Decryption is the same, open the Text Encryption dialog, click back into the window to be decrypted and then click the 'Decrypt' button on the 'Encrypt Window' tab. You will not have to select the key for decryption as DESlock will do this automatically (if the correct key is available)

The text can be decrypted to the DESlock+ Viewer, allowing you to see the plain text but without changing the original document. As above, but click the 'Decrypt to Viewer' button. A new window will open with the decrypted text shown.

Encrypt Selection

As before, open the Text Encryption dialog from the system tray, click back into the window to be encrypted, select the text to be encrypted, and with the 'Encrypt Selection' tab selected in the Text Encryption window, click the 'Encrypt' button. DESlock+ will prompt for an encryption key (or Password/phrase) and then encrypt the selected text and auto paste back into the window.

Decryption can also be performed as before, but the encrypted text must be selected correctly, as shown below, including the DLP BEGIN MSG and DLP END MSG lines.

```
-----DLP BEGIN MSG-----
Encrypted with DESlock+. http://www.deslock.com/email/

I54Mue9HpbD5+YaWMLyyKs4P+uaAvYOrpV1JhFb/C1vVjnkyLc
fkChVuZuhyoU407rF3Ci/KuCoyPKzih31sgRwsiiJMLpohggVW
HeiCjFW6X0kD44ppk+ggMa9UbGrw3Q4FupxTFB+7J1JlmW78Nt
RtkvhfVI2ippRjh2JzfacdVatdJ4joDxHYST1TKUnxe7uXjEY2
qGaUrTKdnMUqh1XCf8XBcn3yGryjzp9/ac2nYs4LiGZPZ72OuZ
myAwhXHZj6XEu+kydoMWdytSEfq7jQxug=QmMvhBZgXNa0ssE/
c6T61lwbgQKbG57ovORftSWozSHoS6RMrrO5f+DDaxYIFCG9
1YwwkY9qCpfhY0ugG1NrGpl6dXLklQOJN2qIFIOQ==
-----DLP END MSG-----
```

The above text has been encrypted with a password (deslock)

The selected text can also be decrypted to the DESlock+ Viewer by selecting the text then clicking the 'Decrypt to Viewer' button.

Encrypt Clipboard

The Text in a window can be encrypted using the windows clipboard and the Text Encryption dialog. Select the text to be encrypted, right click and 'copy'. In the DESlock Text Encryption dialog select the Encrypt Clipboard tab, then click the Encrypt button, select the desired encryption key (or define a password) and click 'OK'. The contents of the clipboard will be encrypted. Use the normal windows paste command to use this encrypted text.

The clipboard can be decrypted in the same way as described in the Encrypt Selection paragraph, but again to see the decrypted text it must be pasted back into a document with the 'Paste' command.

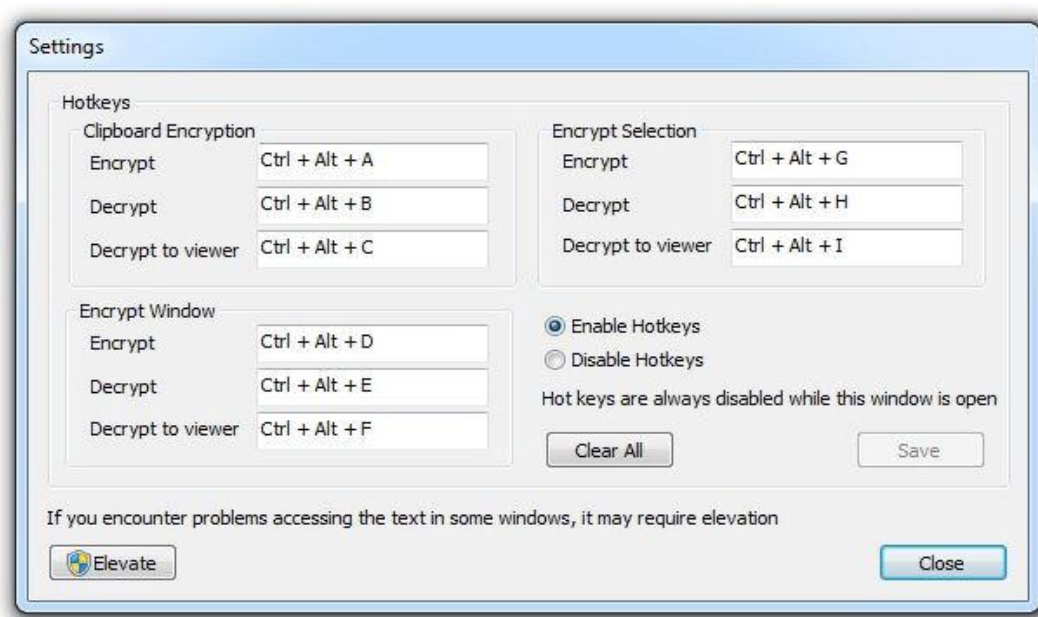
The clipboard can also be decrypted to the DESlock Viewer, by clicking the 'Decrypt to Viewer' button

Settings

The settings window is opened by clicking on the 'Settings' button at the bottom of the Text Encryption window. This enables all the above actions to be specified as "hotkeys", allowing frequent actions to be speeded up and simplified.

Hot Keys

Each key combination has to be defined before it can be used, and the 'Enable Hotkeys' radio button selected.



File Encryption

DESlock+ integrates with Windows to allow encryption and decryption of individual files. This allows files to be encrypted enabling them to be transferred securely, remaining in encrypted format. Please note that this is not the same as [folder encryption](#) as encryption and decryption is not automatic, although the same encryption keys and algorithms can be used in both cases.

This allows files to be encrypted or decrypted after right clicking on them (See below).



File encryption context menu.

The available menu options are:

Encrypt file with DESlock+

If one or more files are selected, and they are all non encrypted, this option will encrypt them all. The user must choose either an encryption key to use for encryption, or must specify a password. If encrypting multiple files at the same time, the same encryption key will be used.

After encryption, the original files will remain intact and encrypted copies will be made in the same folder. The encrypted copies will have a DLP extension and the following icon.



Encrypted file icon.

Decrypt files with DESlock+

If one or more files are selected, and they are all encrypted, this option will decrypt them.



File Decryption context menu

After decryption, the original files can be deleted or left intact. The desired action can be changed in [DESlock+ Settings](#).

Please note that decryption will only occur if the correct encryption key is present in the

currently active Key-File, or the correct password is entered.

Process files with DESlock+

If one or more files are selected, and they are a combination of encrypted and non-encrypted, this option will process them individually following the above rules. That is, if a particular file is non-encrypted it will be encrypted and conversely if it is encrypted it will be decrypted.



Process files with DESlock+

Individual File Encryption is compatible with the Outlook Plug-in, meaning it can be used to send or receive encrypted message attachments with another user using the Outlook Plug-in.

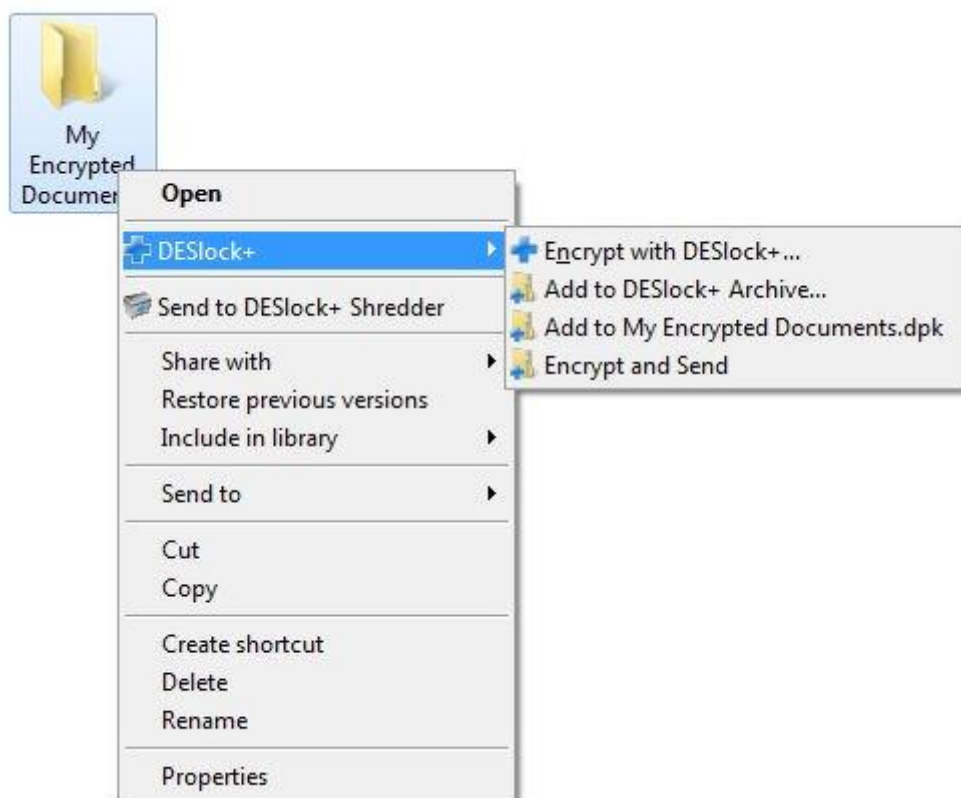
Folder Encryption

The following guide demonstrates encryption of a folder using file system encryption. In this example the folder being encrypted is named **My Encrypted Documents**.



Standard folder icon

Right click on the folder from Windows Explorer and choose **Encrypt with DESlock+...** from the context menu. This will launch the Folder Encryption Wizard which will guide you through the encryption process.



Folder encryption context menu

Please note that not every folder can be encrypted using DESlock+. If DESlock+ determines that a particular folder cannot be encrypted, perhaps because it is a key system folder, then the option to encrypt will not appear. This is to prevent the machine becoming inoperable because folders required by Windows at boot time are made unavailable.

*DESlock+ will also warn the user that a folder may be unsuitable for encryption if it determines that there is a chance the machine **may** be inoperable if the folder was encrypted.*



Folder Encryption Wizard

You must choose an encryption key to use for the encryption of the folder. Any key listed in the key space of the Key-File can be used to encrypt the folder. A password cannot be used to encrypt a folder.

If the only copy of an encryption key is lost there is no way to recover data encrypted using that key. Important keys should be backed up to avoid loss of data. Refer to the [Encryption Key Backups](#) section if you are unfamiliar with the process.



Key selection

Before the encryption begins, a summary screen will be shown with the name of the folder being encrypted, the name of the key being used and the algorithm type. If this is satisfactory, click '**Next**' to begin the encryption process.



Folder Encryption

When ready to encrypt click '**Start**'. As the encryption progresses the icons will turn from their initial state to green. This process may take some time if there are a large number of files in the folder. When complete the folder and all files within, including those within sub folders, will have been encrypted using the specified key. If all tasks were successful, the folder will now be encrypted.



Encryption progress

Once the folder has been encrypted any files copied to, moved to or created in the folder, including sub folders, will be automatically encrypted and protected.

Note that an encrypted folder will have the following icon

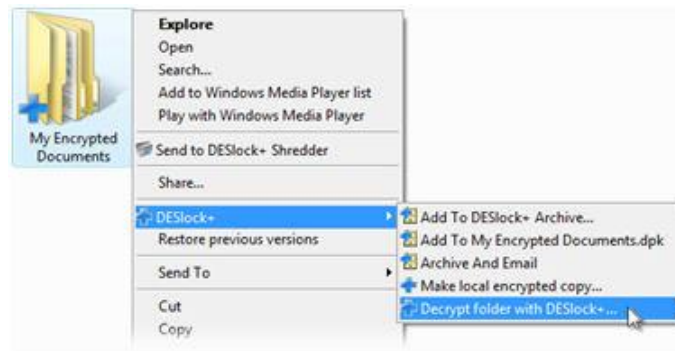


Encrypted folder icon

It is important to note that during the encryption process a copy of the original data will have been made and saved in a folder of the same name but with the suffix DLP Backup. If you do not want this backup to be saved you may uncheck the box on the final wizard screen.

Decryption

If a folder has already been encrypted and you wish to decrypt it and all its contents and subfolders, right click on the folder from Windows Explorer and choose '**Decrypt with DESlock+...**' from the DESlock+ context menu.



Folder Decryption context menu

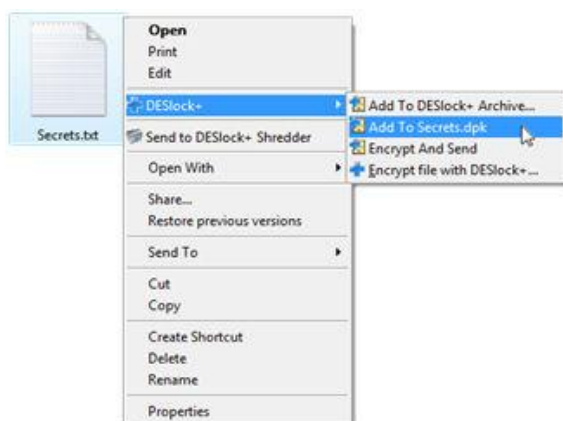
Encrypting Network Shares

It is not possible to encrypt a folder on a network drive. For network drives, you should use a DESlock+ Virtual Disk. The file can reside on a network location and can be mounted from there when necessary. See [DESlock+ Virtual Disk Manager](#) for more details.

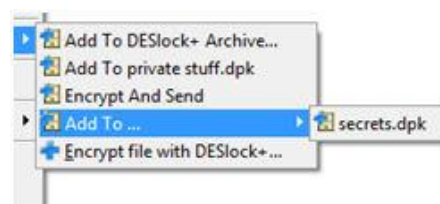
Archive

The DESlock+ Archive allows a number of files to be stored in a compressed, encrypted archive.

Archive options are available from the DESlock+ context menu, when right-clicking on a suitable file. See below, left.



Standard context menu



enhanced context menu

Note: If the file exists in a folder containing an existing archive, the enhanced context menu will show an additional menu item of 'Add to' with a list of all archives in that folder. See above right.

The available options allow the user to:

- **Add to DESlock+ Archive** – Add the file to a new archive and then prompt to save it in a specified location.
- **Add to filename.dpk** - Add the file to an archive of the same name as the file, in the same folder.
- **Encrypt and send** – with this you can:
 - Add the file to an archive and then attach it to an email, or:
 - Send the file as an encrypted file.Please see [Encrypt and Send](#) for details of these sub options:
- **Add to** – Adds the file to available archives (as listed) in the current folder.
- **Encrypt the file** – Encrypts the file, see [file encryption](#) for more details

When an archive is created for the first time, an encryption key must be chosen. You may also use a Password for the Archive. This encryption key (or password) will be used to encrypt all files in the archive.



Click 'OK' to continue. The Archive will be created in the same folder as the file you originally clicked, if the 'Add to filename.dpk' option was chosen; if 'Add to DESlock+ Archive' was selected the file will be saved in the folder specified.



To Open the Archive, double click the Archive file and the DESlock+ Archive window will open (below)



Archive

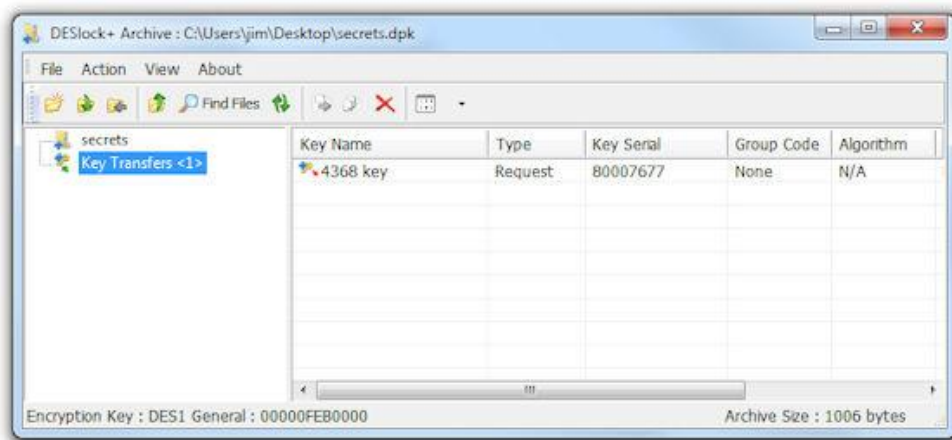
Once open, files may be added or removed using the normal windows drag and drop or copy/paste as with normal file movements.

The Archive may now be used by any DESlock+ user who has access to the file (via a network, mail etc) and the correct encryption Key (or the Password)

If the archive has been created with an encryption key that the intended recipient does not have, it is possible to include the encryption key based on a key request from the recipient's Key-File. This request can be generated using the [Key Transfer Wizard](#). The key update can then be created and attached using the **'Add key update using request file'** on the Action menu.

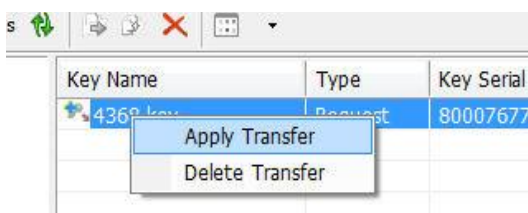
Alternatively key updates can be dragged and dropped on the archive window.

If any encryption keys have been included with the archive, these will be available under the key transfer section.



Archive, key transfers

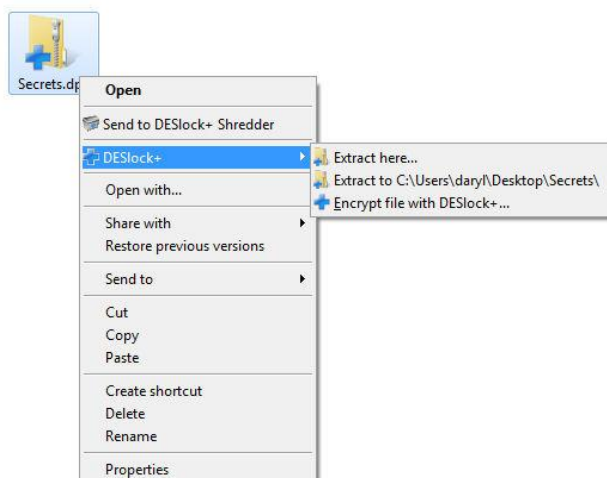
To import the encryption key, right click on the key and choose '**Apply Transfer**' from the context menu



Key transfer

This will then launch the update phase of the Key Transfer wizard. If the encryption key is not available in the currently active Key-file (i.e. it has not been imported), the files in the archive will remain inaccessible.

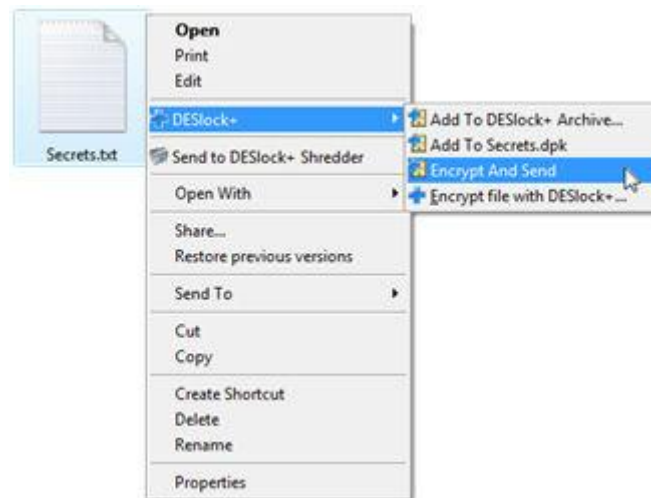
To extract files from a DESlock+ Archive, one can either drag the files out from the main window into the desired folder, or one may choose to extract the files using the context menu.



Archive file extraction

Encrypt and Send

The DESlock+ Context menu allows the selected file (or files) to be encrypted and emailed in a simple operation.



Encrypt and send

Depending on the system policy, either the user will be prompted to choose the type of email attachment to create or it will be automatically selected.

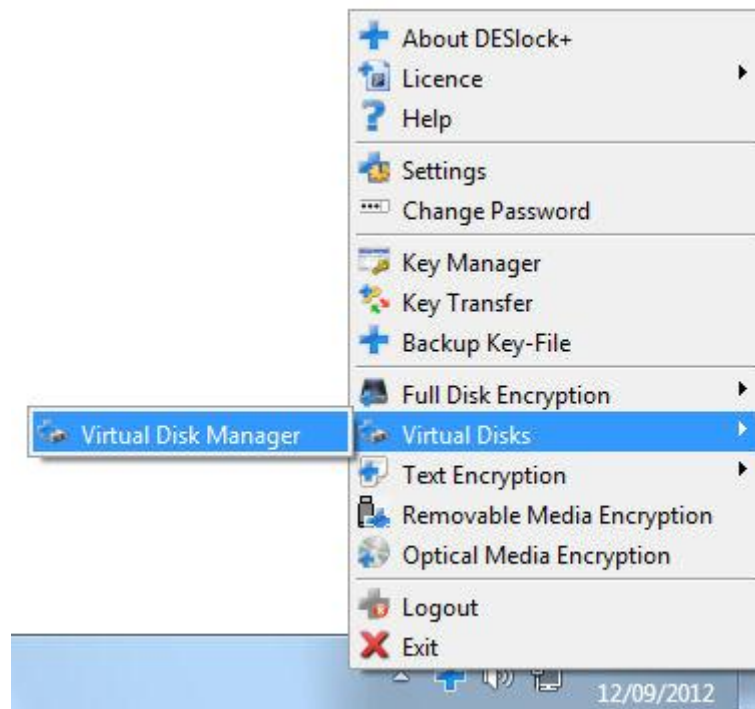


Encrypt and send options

Virtual Disk Manager

The DESlock+ Virtual Disk Manager is designed to allow a special type of DESlock+ encrypted file to be mounted by Windows and accessed as a normal volume or drive. Such an encrypted file is designed to be placed on any existing media, be it an existing local drive, a network drive or removable media. It can also be used in any location where standard DESlock+ folder encryption is not desired or is not suitable.

The DESlock+ Virtual Disk Manager program is accessible via the DESlock+ System Tray menu.



DESlock+ Virtual Disk Manager

Virtual Disk Manager Functions



Options are:

Create

See [Creating Virtual Disks](#) for details.

Import

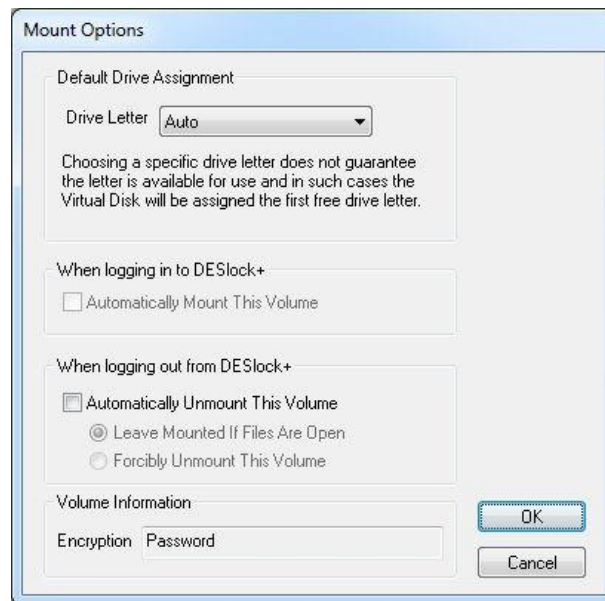
DESlock+ Virtual Disk Manager maintains records of Virtual Disks accessible from your PC. You cannot mount a Virtual Disk until it has been imported into the Virtual Disk Manager. If you copy a new Virtual Disk to your PC, or need to access one on a network, either double click the file (which opens the Virtual disk manager then imports it) or use the import function to add the Virtual Disk file to the Virtual Disk Manager. The Import button opens a windows explorer window allowing you to browse to the Virtual Disk File location. Click on the file name and then select 'Open'. The Virtual Disk will appear in the Virtual Disk Manager and can then be mounted.

Mount/Unmount

This allows a Virtual Drive to be Mounted or unmounted, with the action changing depending on if the highlighted drive is already Mounted or not. i.e. if the drive is unmounted, the option will show 'mount' and vice versa.

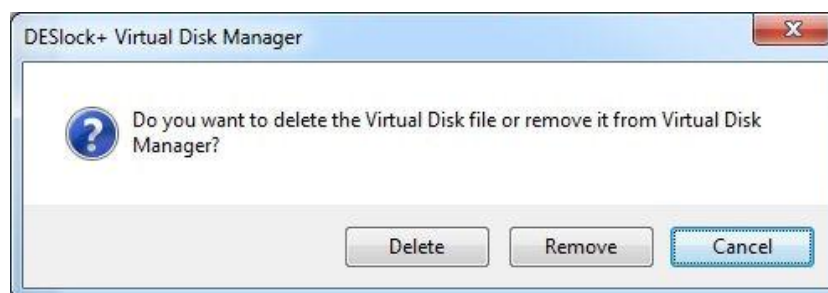
Options

This allows the options for the Virtual Disk file to be modified. This includes the assignment of a preferred drive letter, or the 'Auto' option allowing windows to allocate the first available drive letter. You can also define the actions taken when logging into and out of DESlock+ (Auto mounting and unmounting)



Delete

Gives you the option of either Deleting the Virtual Disk file or removing it from the Virtual Disk Manager. If you select **Delete** the file will be deleted as well as any files or data it contains. **Remove** only removes the reference to the Virtual disk from the Virtual Disk Manager, no data is affected. To Delete (or remove) a Virtual Disk, highlight the entry in the list then select delete. At the next window select **Delete** or **Remove** as necessary.



Rename.

Allows you to rename a Virtual Disk file. Highlight the Entry to be renamed and click '**Rename**'. The name in the Entries window will become editable. Change the text as required and press return.

Refresh

Refreshes the entries in the window.

Inaccessible Drives

In the Virtual Disk Manager window at the start of the section, the greyed out Virtual Disk is not accessible to the Virtual Disk Manager. Virtual Disks may be not accessible either due to the path being incorrect, the file not being at the specified location, or, the Encryption key required for it not being available.

Creating Virtual Disks

To create a Virtual Disk file, run the Virtual Disk Manager application. Click the '**Create**' button to create a new Virtual Disk file. To open an existing Virtual disk select the disk in the main window and then select '**Mount**'. If a disk is not listed (because you have copied it from another location for example) it will need to be imported. DESlock+ maintains location information on existing virtual disks.



DESlock+ Virtual Disk Manager

When creating a new file, you need to define the type of Virtual disk required. You can choose from either an;

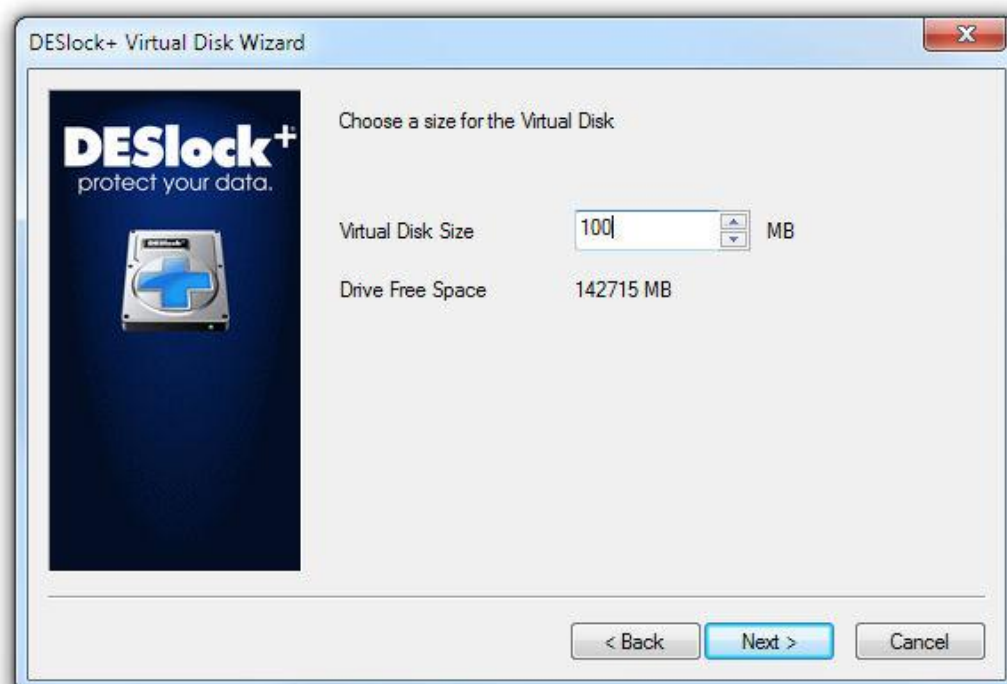
- Enhanced Virtual disk, which uses a "Sparse" File - these files only grow in size as the virtual disk space is filled, up to the maximum size you have specified, Windows will always list the maximum size, but the actual file size will be only the space used on the disk.
- Standard Virtual disk. These are compatible with older versions of DESlock+. The file size on your HDD will always be the size defined during the creation of the virtual disk.

To create a virtual disk, define the file type required, then enter a file name and location to store the file.



DESlock+ Virtual Disk Wizard.

Next, you must enter the attributes of the file (See Figure below). The **Virtual Disk Size** setting specifies the size of the drive that this file will provide. By default, this will be 10% of the available space on the hard disk the file is located; The minimum disk size is 10MB. This value cannot be modified once the file has been created.



Virtual disk Attributes

Then choose whether to encrypt the Virtual Disk with an encryption key or a password. Select the Key (highlight the required slot and click Next) or define the password when prompted.



Next choose the drive options. These options can be modified again after the Virtual Disk file has been created.



Virtual Disk options

The **Default Drive Assignment** option allows the user to specify which drive letter the Virtual Disk file will be mounted at. This setting is stored within the Virtual Disk file itself, so care should be taken in choosing a drive letter if the Virtual Disk file will be used in a shared environment.

The **Automatically Mount This Volume** option directs DESlock+ to attempt to mount the Virtual Disk when a user logs into DESlock+ and the correct encryption key is present. This is not applicable if the volume is protected with a password as these must be mounted manually.

The **Automatically Unmount This Volume** option directs DESlock+ to attempt to unmount the volume when the user logs out of DESlock+.

By choosing the relevant option, the unmount can be deferred if DESlock+ detects that any of the files stored on the drive are still open or it can forcibly unmount the drive even if files are still open.

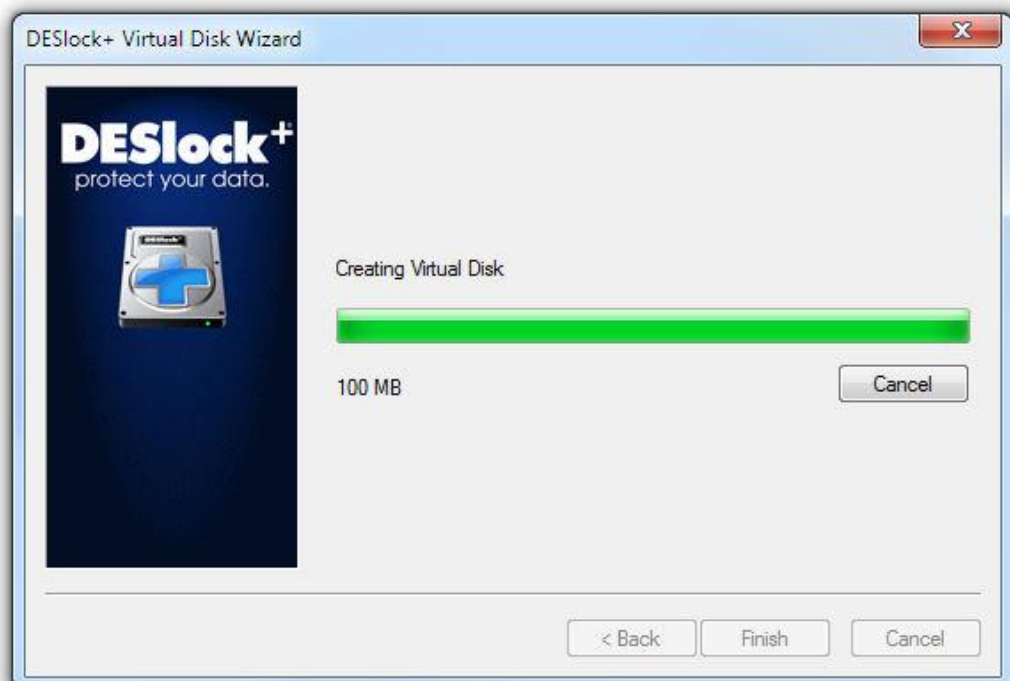
Summary

Once a suitable Filename, location, Encryption key (or password) and options have been chosen, the Wizard will show a summary screen.



Mount file parameters.

If all details are correct, click '**Next**' to accept the parameters, and the virtual disk will be created.



And, once the process has completed, click finish. If the 'Mount Virtual Disk' check box is selected then Windows Explorer will open showing the virtual disk drive.



When the file has been mounted, (either Auto mounted or mounted through the Virtual Disk Manager), it will appear as a new drive in Windows Explorer and can be accessed and used in the same way that any other drive would be. Note that the Disk Icon (Local Disk (E:)) in the example) includes the DESlock+ symbol to denote that the disk is encrypted.



Once the entry appears in the Virtual Disk Manager, the file may be mounted and unmounted in future from the DESlock+ system tray menu. Also other tasks may be performed on the Virtual Disk, see section [Using Virtual Disks](#) for details.

Using Virtual Disks

DESlock+ Virtual Disks provide a virtual drive on the PC on which the file has been mounted. The file itself can be stored on any location accessible by the PC, either on a local drive or on a network path.

Shared Access

If the file is stored on a network path it can be mounted and unmounted as if it were a local file. However, because it is in a shared location, it is possible that another user could also access the file at the same time. If two users attempt to mount the file at the same time, then only one (the first) will be successful in mounting the file with read and write access to the drive. Any additional users who then mount the file will only be able to access the drive with read access.

Users with read access to the volume will be able to access files within and will see changes made to them, but will not see changes made to the file system, such as new files or folders being added. A user must unmount the drive and remount it to see any changes to the file system.

Windows File and Sharing

DESlock+ cannot be used to directly encrypt a folder that is shared with Windows file sharing, however a folder within a DESlock+ Virtual Disk may be shared. Standard share permissions can be used on the folder meaning multiple users can share write access to the folder. However, while the share is active, the volume cannot be unmounted.

Important Notice

Encryption Key Caching

Please be aware that the DESlock+ Virtual Disks work differently than the standard encrypted folders in that the required encryption key is cached for the duration the drive is mounted.

This means that performance of the drive is faster than it would be with a normal encrypted folder.

However, it means that the drive may continue to be available on your PC even if DESlock+ is deactivated. The automatic unmount option can be used to attempt to unmount the drive on deactivation of DESlock+.

The encryption key is only required to mount the drive, but once mounted files can be accessed without using DESlock+ again. This means the files are accessible until the drive is unmounted.

Please be aware therefore, that once mounted, and until the drive is unmounted, **any user of your PC can access the drive even if DESlock+ has been deactivated.**

Removable Media Encryption

DESlock+ Removable Media Encryption allows encryption of removable devices such as USB memory sticks, flash drives or USB Hard Disks.

Overview

DESlock+ Removable Media Encryption is controlled by policies set within the Key-File or on the workstation.

In a managed environment workstation policy can be used to restrict or control access to non-encrypted memory devices. Policy can be set to Open - any removable media device is allowed, Blocked - access to removable devices is blocked or Read Only- where the devices can be read but not written to.

On a standalone system, when logged into DESlock+, Key-File policy controls access. If the removable media device is not currently encrypted, the user may be prompted to encrypt the device if required. In a managed environment, this choice may be forced upon the user by system policy.

As with any other DESlock+ feature, encryption and decryption functions will only be performed if DESlock+ is installed and the user is logged in.

One important exception to this is [DESlock+ Go](#), where Licenced DESlock+ users can allow access to encrypted data on removable devices to selected persons through the use of passwords. Data will be accessible if the password is known and DESlock+ Go is used, or if DESlock+ is installed and the correct encryption key is held.

Encryption Methods

There are two methods of encryption of removable media, which gives maximum flexibility on how the removable media is used.

Full Disk

With this method the entire memory device is encrypted. The benefit is that any existing data on the device is automatically encrypted, and the device is completely unusable on a system without DESlock+, or without the correct encryption key available. All data added to the device is automatically encrypted and decrypted when removed.

For details of the process steps see [RM Full Disk Encryption](#).

File

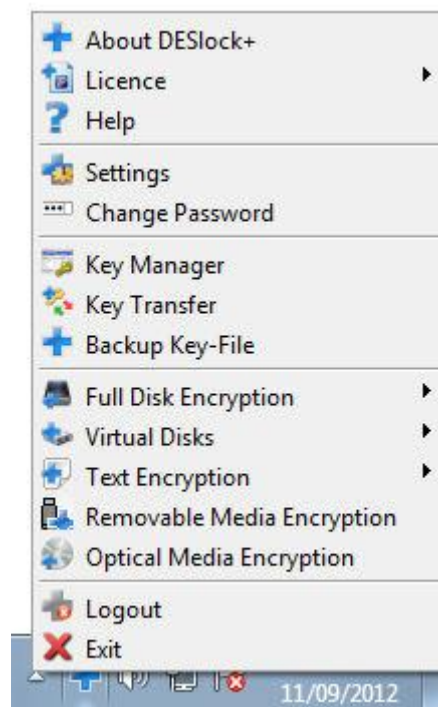
With this method the memory on the device is divided into two distinct encrypted and non encrypted areas. Any data that already exists on the device while it is being encrypted will remain decrypted. Once the encryption process has been completed, any data added to the encrypted section of the device will be automatically encrypted and decrypted when removed. The remainder of the device may be used as normal.

During the encryption process DESlock+ Go may be selected for use on that removable device. DESlock+ Go is only available for removable devices encrypted in File Mode.

For details see [RM File Mode Encryption](#)

Removable Encryption Access

Both types of removable media encryption are available through right clicking on the DESlock+ icon in the system tray (as below), or on insertion of a USB device when encryption options will automatically appear.



Removable Media Full Disk Encryption

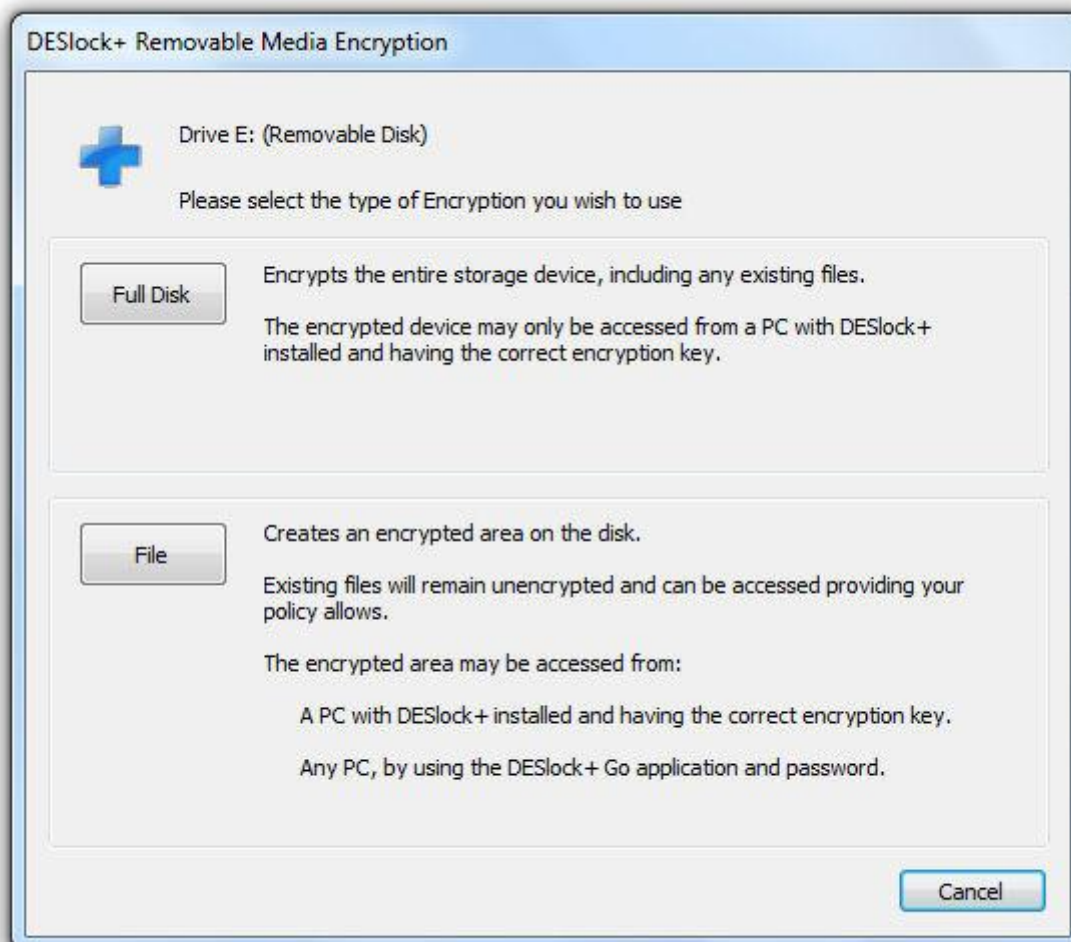
1. Insert your USB Memory device (Flash memory, USB Hard Drive), DESlock+ will read the device and if it is not encrypted (either with Full Disk or File mode Encryption) it will display the message below. Select 'Yes'.



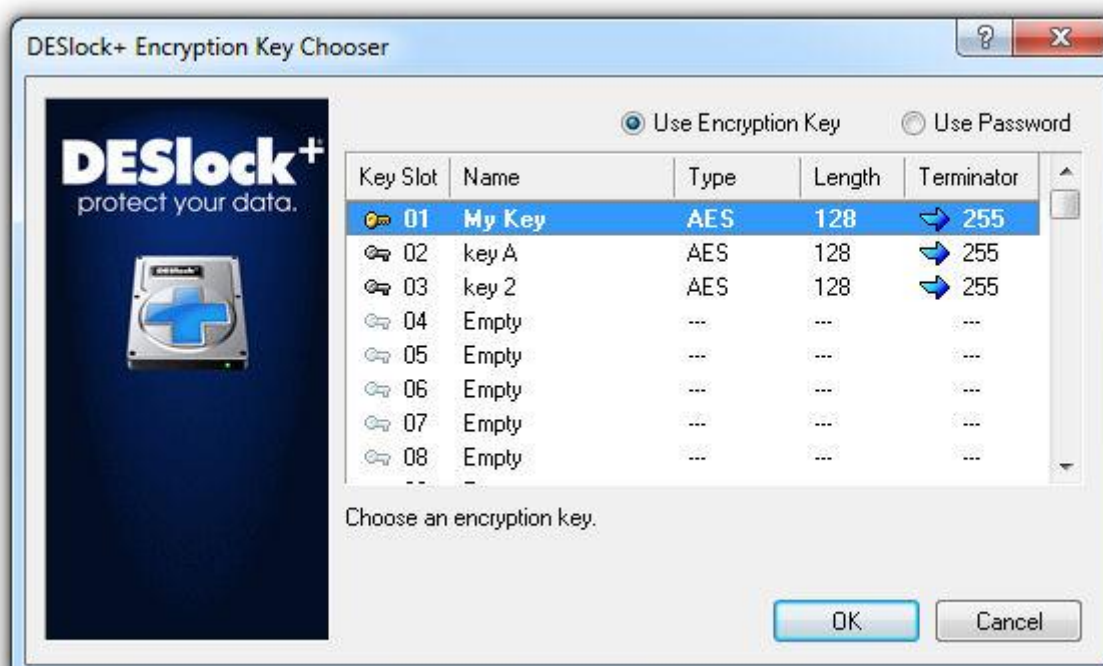
2. Note: If you are not logged on to DESlock+ you will get a message informing you that an unencrypted drive has been connected, and giving you the option to login.



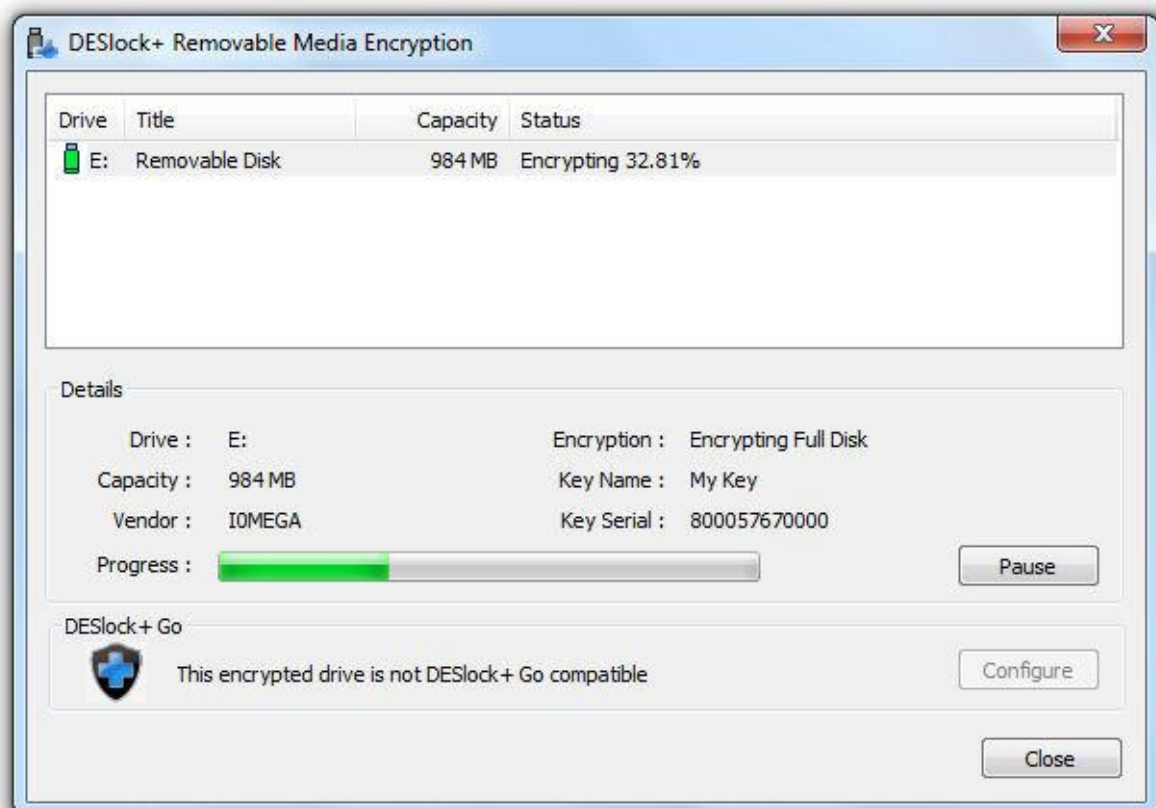
3. Choose the type of Encryption required. Select 'Full Disk'.



4. Select which Encryption Key is required. Click 'OK'.



5. Encryption will now start, once you click 'Yes'. Make sure you do not remove the memory device during encryption.



6. On completion, a brief message will show, as below.



7. The Memory device will now be able to be used as normal, as long as you are logged in to DESlock+. Any files or folders added to the Memory device will be encrypted, and any data removed will be decrypted.

Removable Media File Mode Encryption

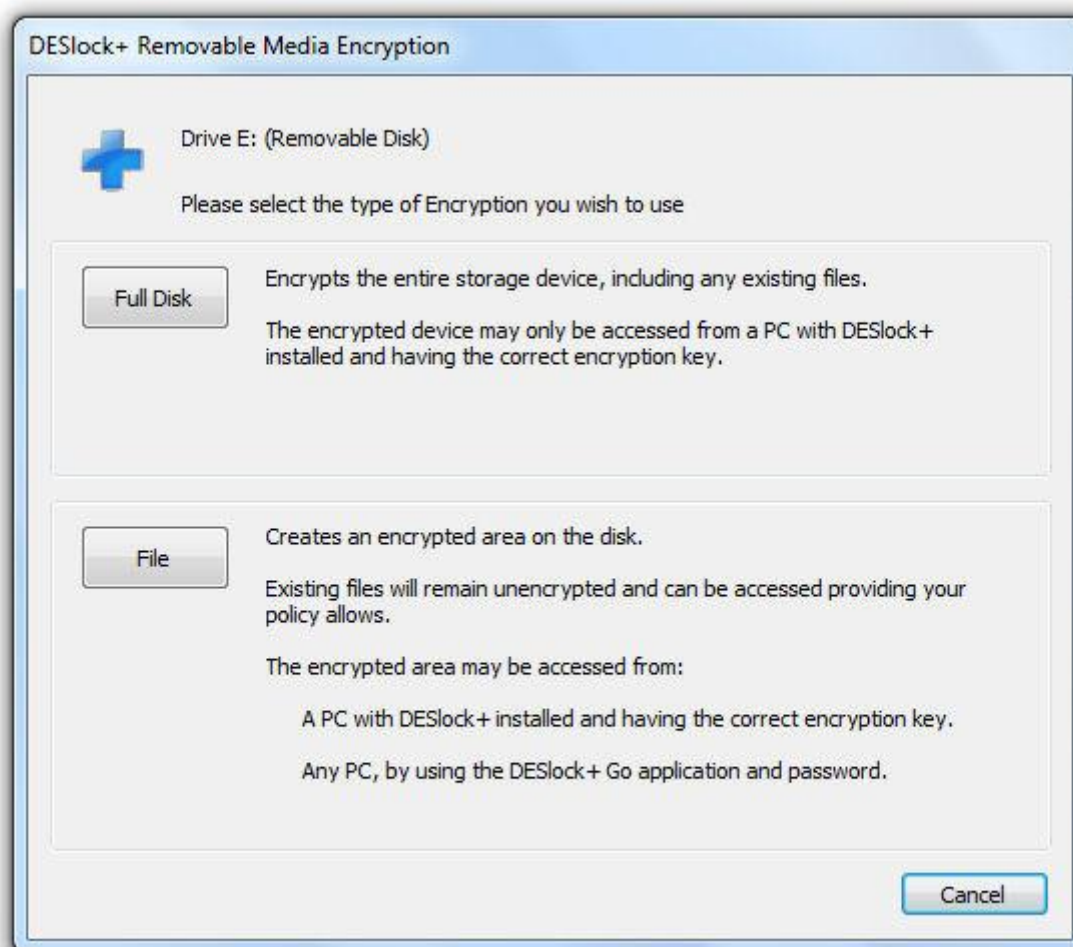
1. Insert your USB Memory device (Flash memory, USB Hard Drive), DESlock+ will read the device and if it is not encrypted (either with Full Disk or File mode Encryption) it will display the message below. Select 'Yes'.



2. Note: If you are not logged on to DESlock+ you will get a message informing you that an unencrypted drive has been connected, and giving you the option to login.



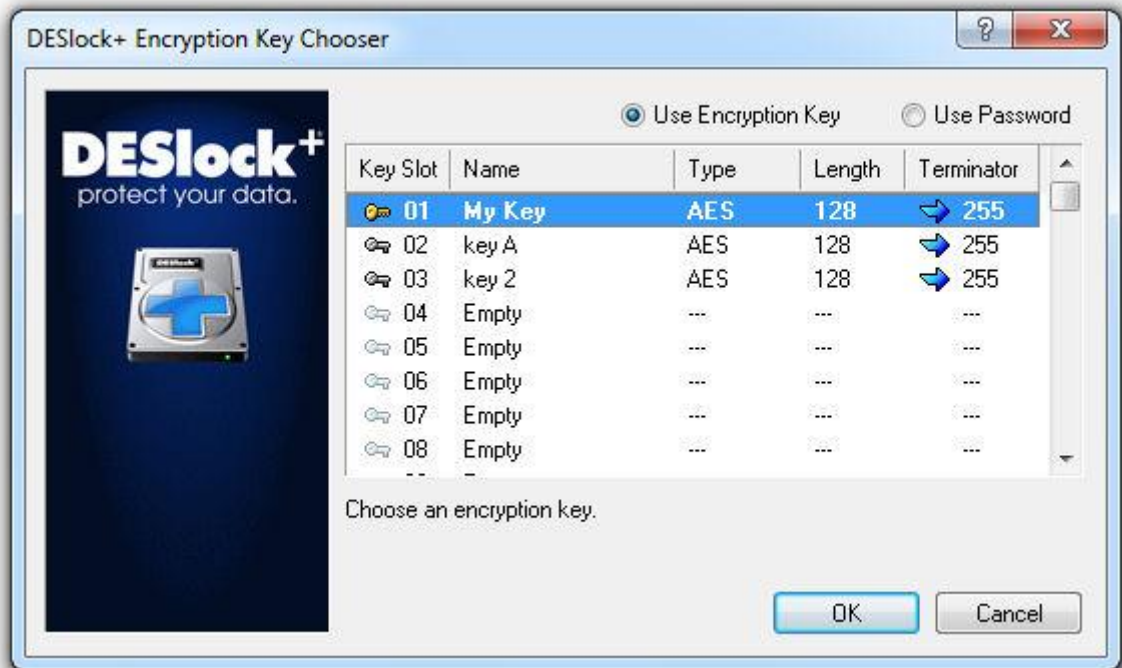
3. Choose the type of encryption required. Select 'File'.



You may also get to the above window by right clicking 'Removable Media Encryption' in the system tray.



4. Select which encryption key is required. Click 'OK'.



5. With file encryption, you also have the option of enabling DESlock+ Go. This allows the memory device to be used with a password, whether or not DESlock+ is installed on that system. Select 'Yes' to enable DESlock+ Go, or 'No' to use file encryption alone. For more details on DESlock+ Go see the [DESlock+ Go](#) chapter.



6. If you enabled DESlock+ Go, you will now need to enter a password. Enter this twice and click 'OK'.



The screenshot shows a Windows-style dialog box titled "Choose a Password for DESlock+ Go". It features a shield icon with a blue cross. There are two text input fields: "Enter a password" and "Confirm the password". Below these fields are two checkboxes: "Show Typing" and "Disable DESlock+ Go after 5 password attempts". The number "5" is in a small spinner box. At the bottom right are "OK" and "Cancel" buttons.

7. The memory device will now be configured to enable file encryption and DESlock+ Go (if selected)



The screenshot shows a Windows-style dialog box titled "DESlock+ Removable Media Encryption". It features a blue plus icon. The text inside reads: "Drive E: (Removable Disk) Encryption has now been setup" and "The drive is now available and can be used as normal". At the bottom right is an "OK" button.

8. Once completed, the memory device will have an encrypted folder, and the remainder of the drive will be available for you to store unencrypted (plain) data. If you selected to use DESlock+ Go the DESlock+ Go program will be added to the Drive (dlpgo.exe).

Optical Media Encryption

Overview

DESlock+ Optical Media Encryption allows encrypted files to be burned and accessed on CD's and DVD's. All the data on the CD/DVD is encrypted.

DESlock+ Optical Media Encryption is available on all licence types, with the exception of the Free Personal Licence.

To use Optical Media Encryption you simply follow the Optical Media Encryption wizard, which takes you through selection of the files to be encrypted, the encryption key to be used, and if you are permitting DESlock+ Go access to the encrypted media. Once these choices have been made, the wizard burns the files to the disk. To view the files, insert the DVD/CD into the drive and open the encrypted folder.

As with all DESlock+ features, Optical Media Encryption files can only be written to the CD/DVD when you are logged into a licensed copy of DESlock+. Files can be read on any computer with DESlock+ installed which also has a copy of the encryption key used to encrypt the data.

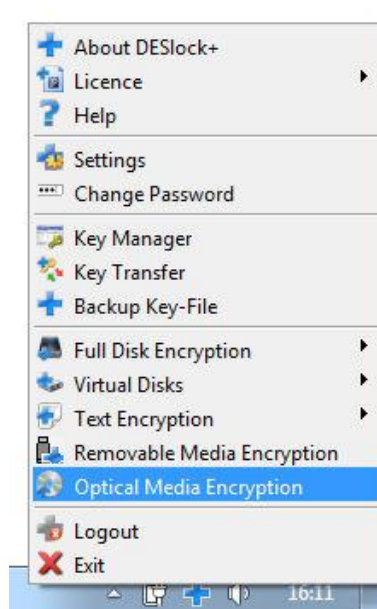
One important exception to this is [DESlock+ Go](#), where Licenced DESlock+ users can allow access to encrypted data on Optical Media to selected persons through the use of passwords. Data will be accessible if the password is known and DESlock+ Go is used.

You cannot add data to encrypted folders once they have been burned to a disk.

Writing Data to Optical Media

To create an Encrypted CD/DVD

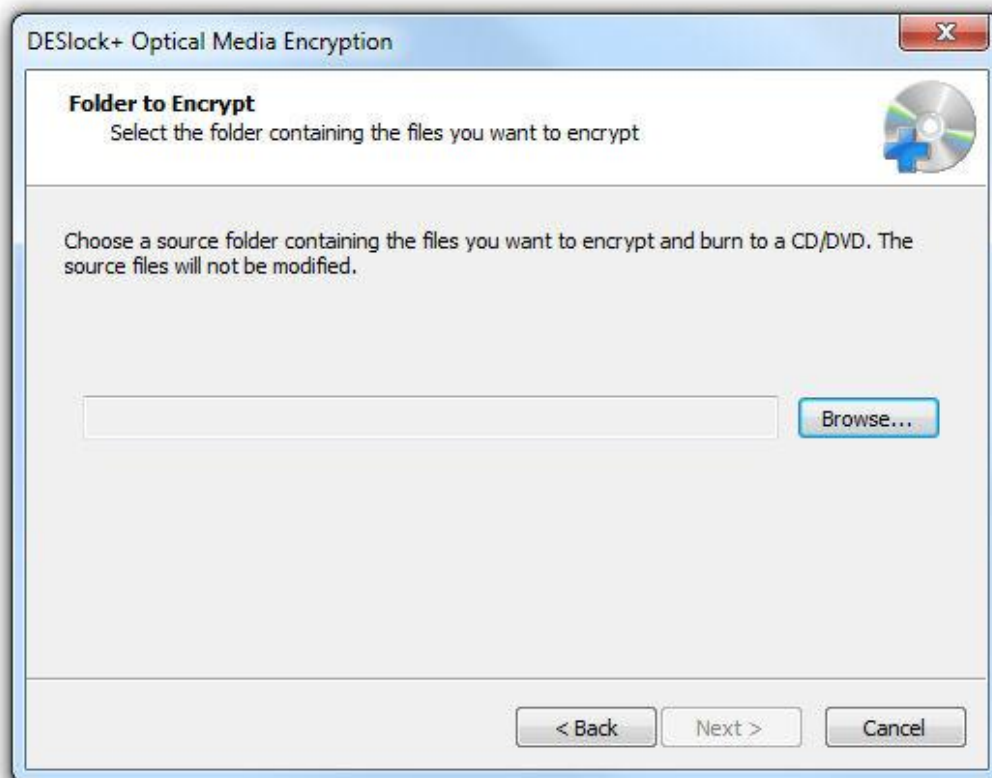
1. Right click on the DESlock+ icon in the system tray.
2. Select 'Optical Media Encryption' as shown below.



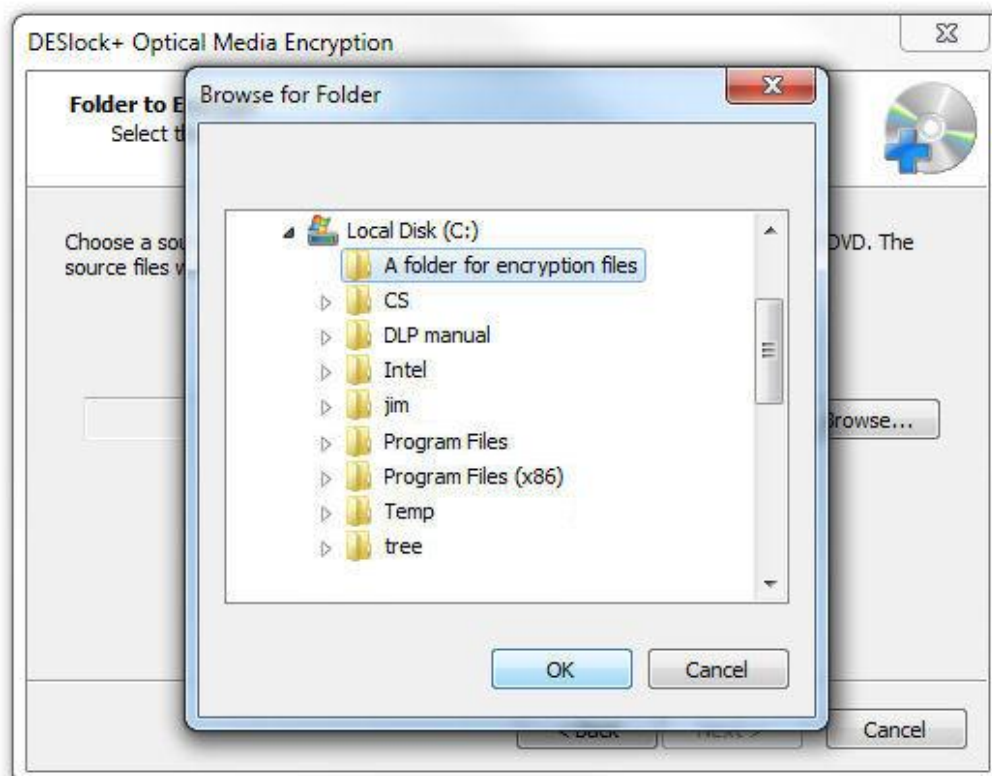
3. This will open the Optical Media Encryption Wizard. Click 'Next' to continue



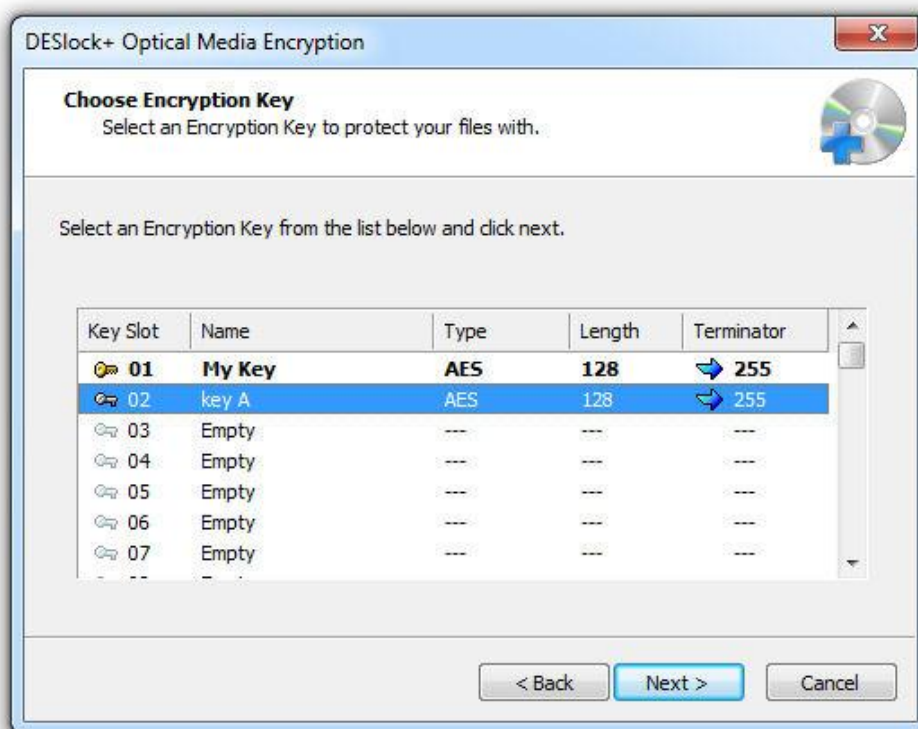
4. Then select the folder containing the data you wish to encrypt.



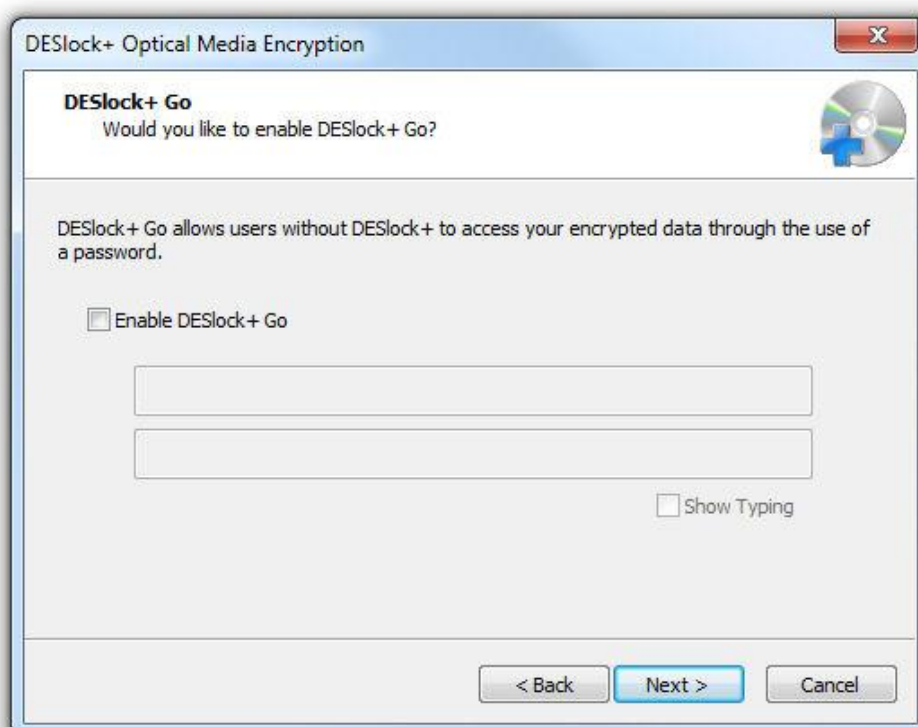
5. Navigate to the location of the folder that contains the data you want to encrypt, and click 'OK'.

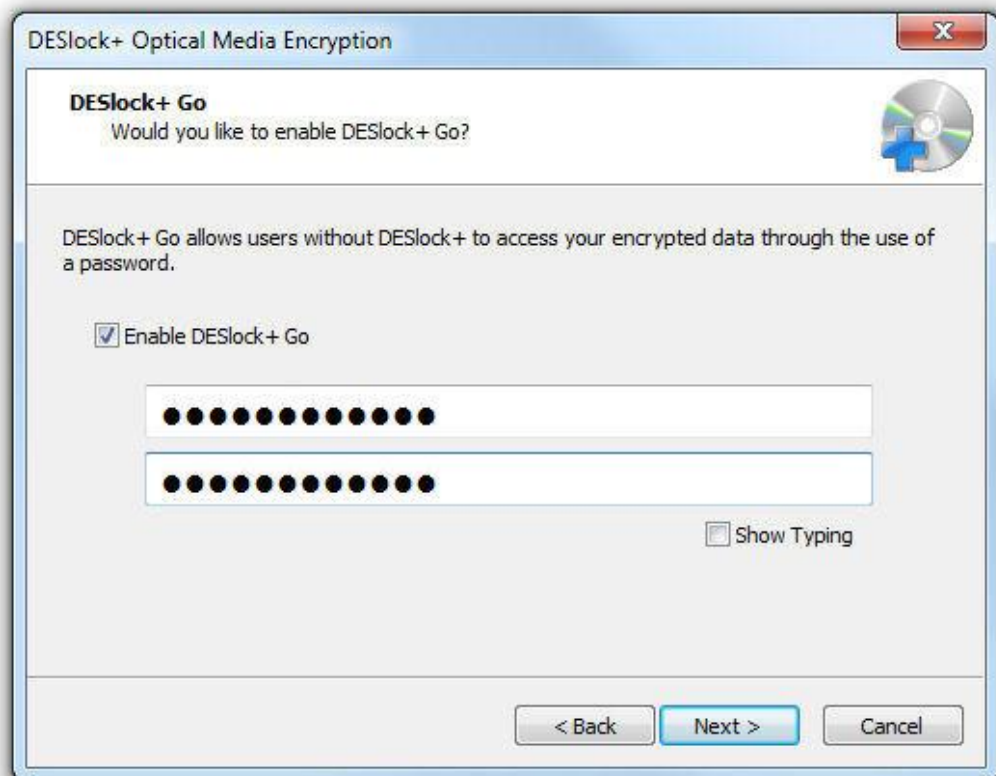


6. Then select a key for the encryption process. Once selected click 'Next'.

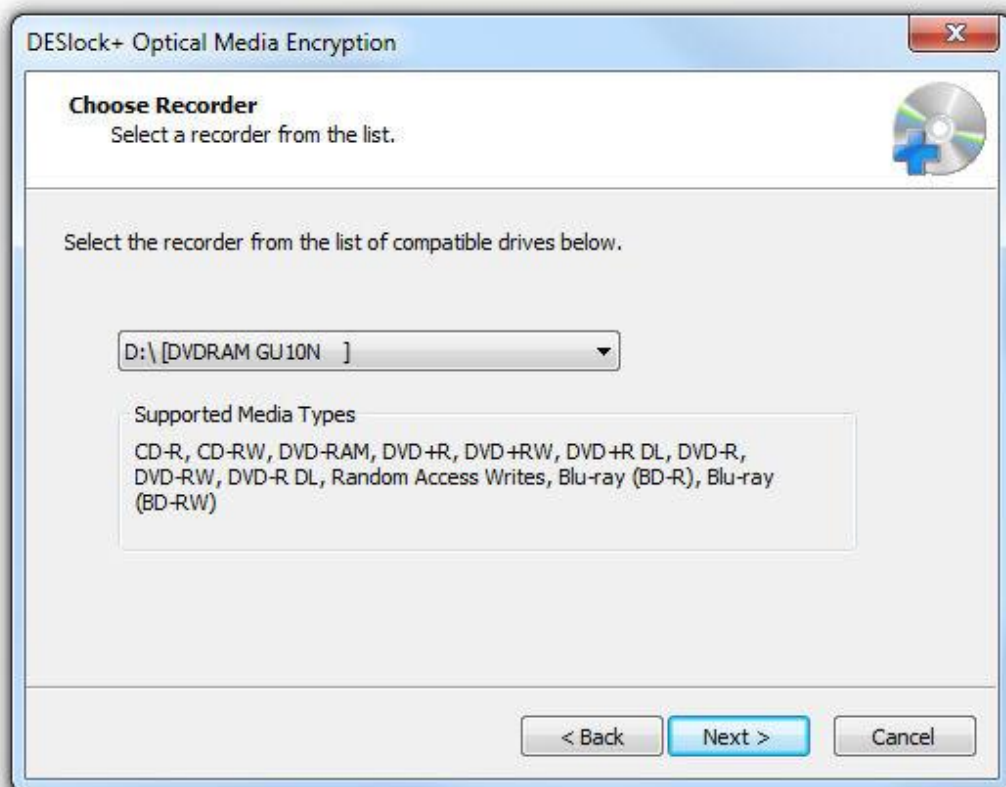


7. This window allows you to define if DESlock+ Go is to be enabled on the CD/DVD. This will allow access to the encrypted data by anyone who knows the password. If you wish to use DESlock+ Go, check the tick box and enter the required password or phrase.

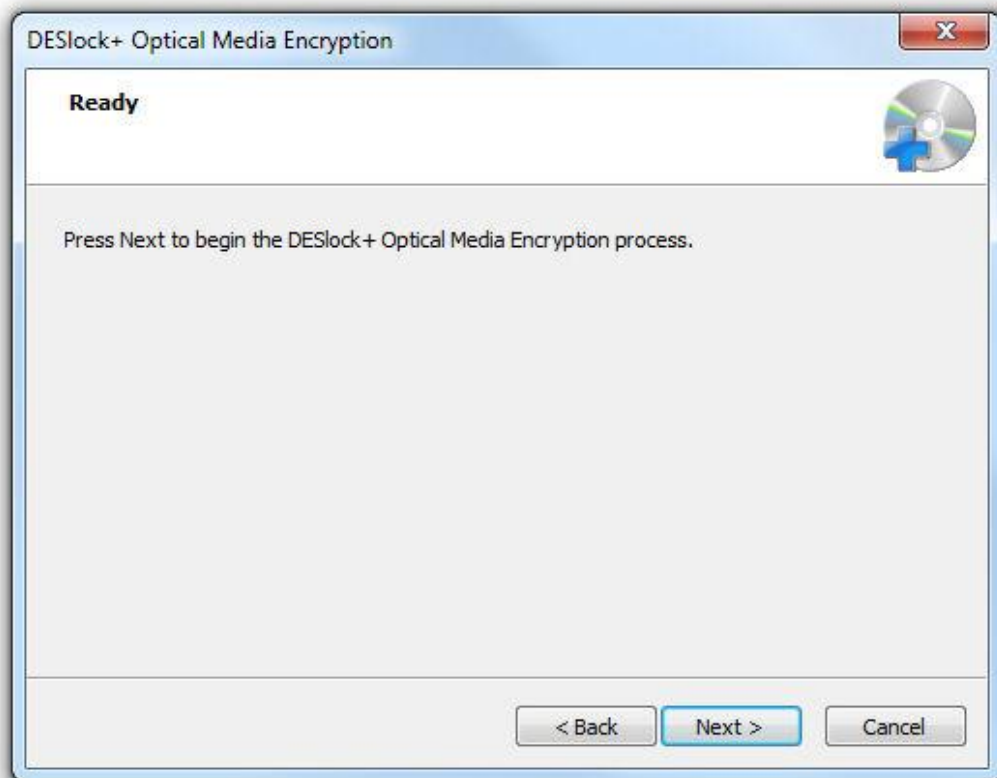




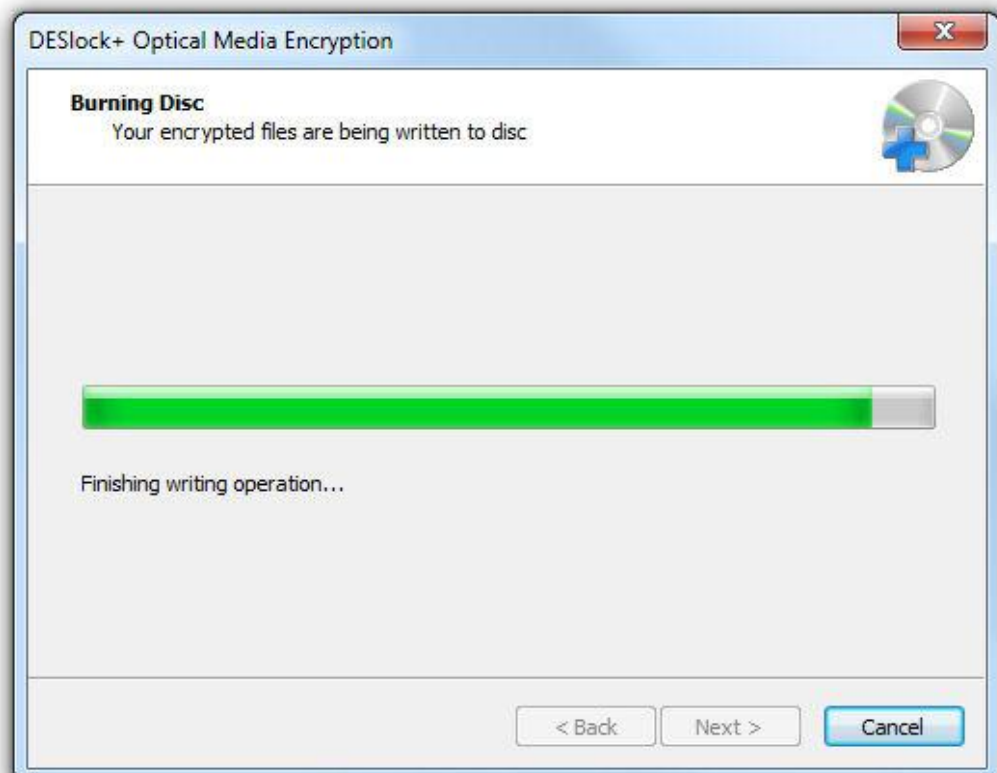
8. Select the drive you wish to use - on most systems there will only be one drive. Click 'Next'.



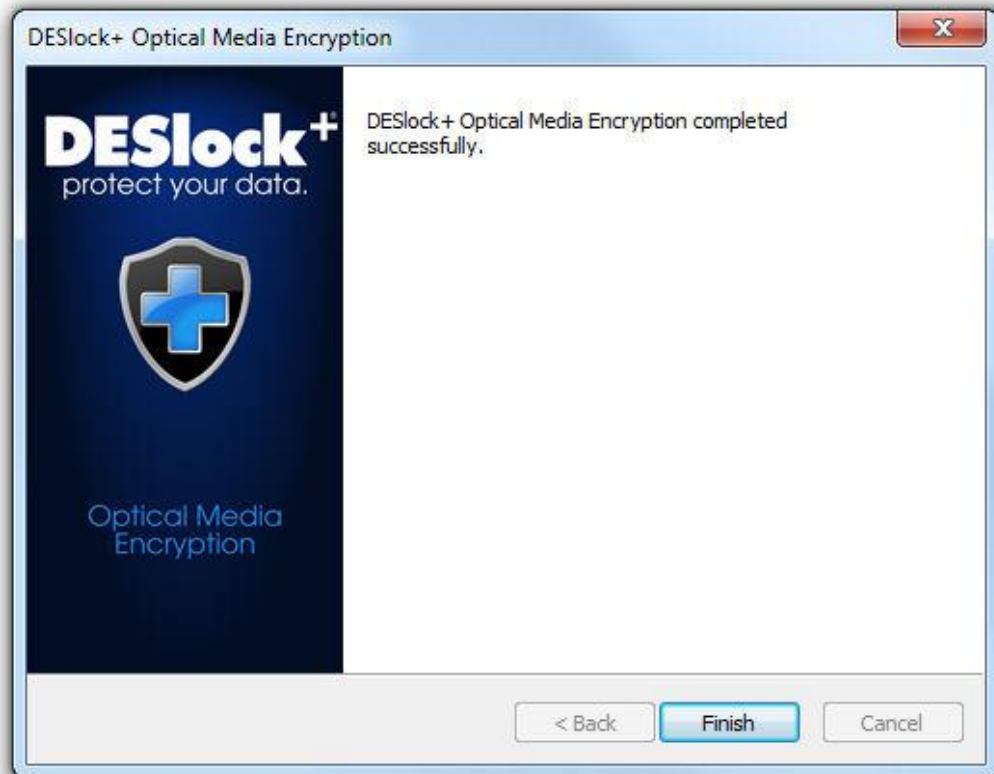
9. Once all the parameters have been defined, click 'Next' to start writing the data to the CD/DVD. Make sure you have media in the drive.



10. The Data will be written to the DVD/CD



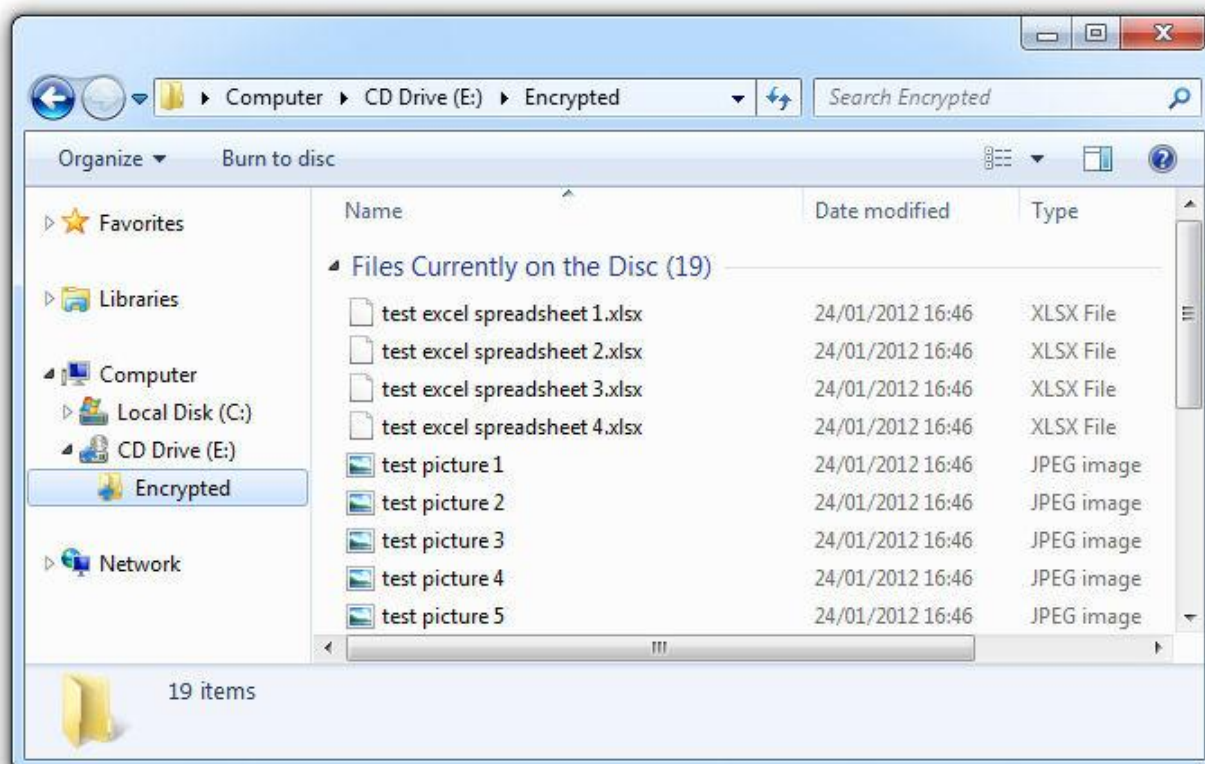
11. On completion, the DVD/CD will be ejected from the drive and the window below will display. Click 'Finish' to close the wizard.



Reading Data from Optical Media

To read data from an Encrypted DVD/CD;

1. Insert CD/DVD into the drive
2. Windows explorer may open automatically (which is dependent on your Windows Settings), but if it does not, open it.
3. The Encrypted CD/DVD drive will appear with a small blue cross (DESlock+ icon) - CD Drive (E:) in the example.
4. Expand this drive and you will see an encrypted folder and a subdirectory.
5. Select this, and the files contained will be displayed.



6. Files can be opened and read, but cannot be saved back to the Optical Media.

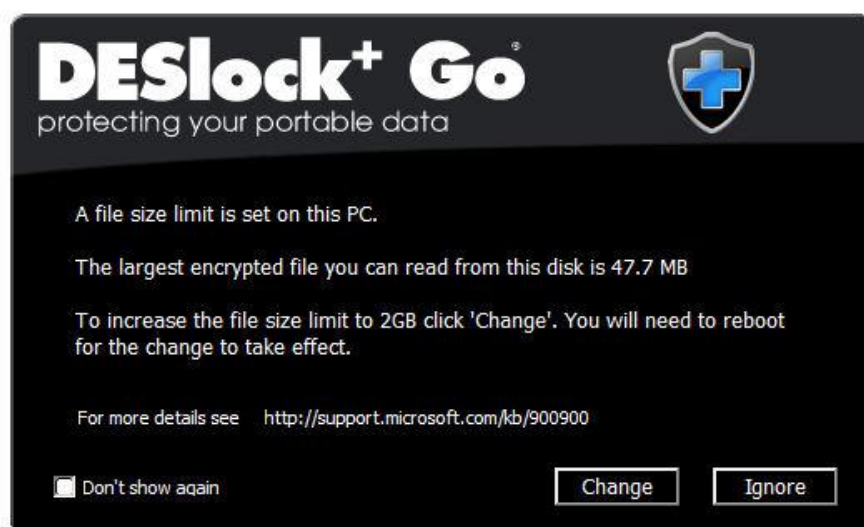
Reading Optical Media with DLP Go

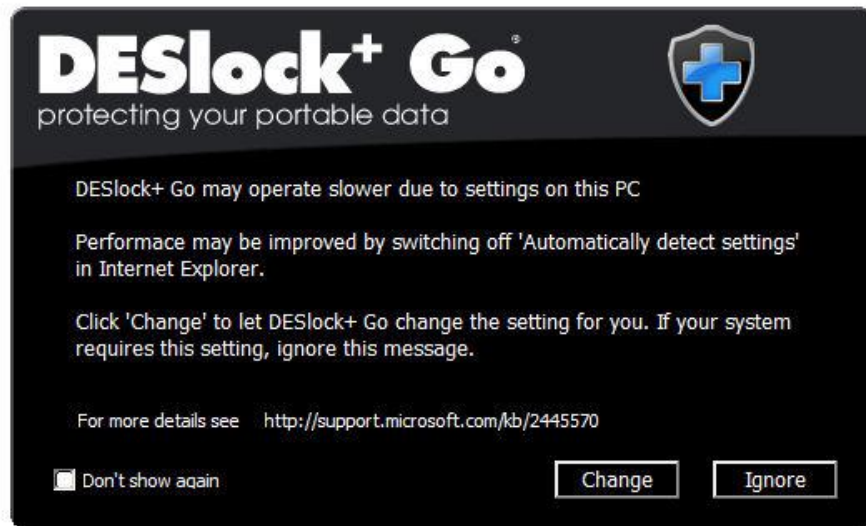
Reading Optical Media using DESlock+ Go on a computer without DESlock+ installed is described below. This enables a licensed user to share data securely with any other person. If the CD/DVD is attempted to be used without the correct password, access will be restricted after 3 attempts.

1. Insert the Encrypted Optical Media into your drive.
2. If Windows AutoPlay is used on your machine the following message will display. If this happens, click 'Access Encrypted Files'.



3. If AutoPlay does not run, open windows explorer and select the drive containing the Encrypted Data. Double click the Drive letter.
4. DESlock+ Go will start automatically.
5. Depending on the machine settings, the following warnings may be displayed, these can be ignored for the purposes of reading the data.





6. After these information messages, the DESlock+ Go Password window is displayed. Enter the password associated with the Disc.

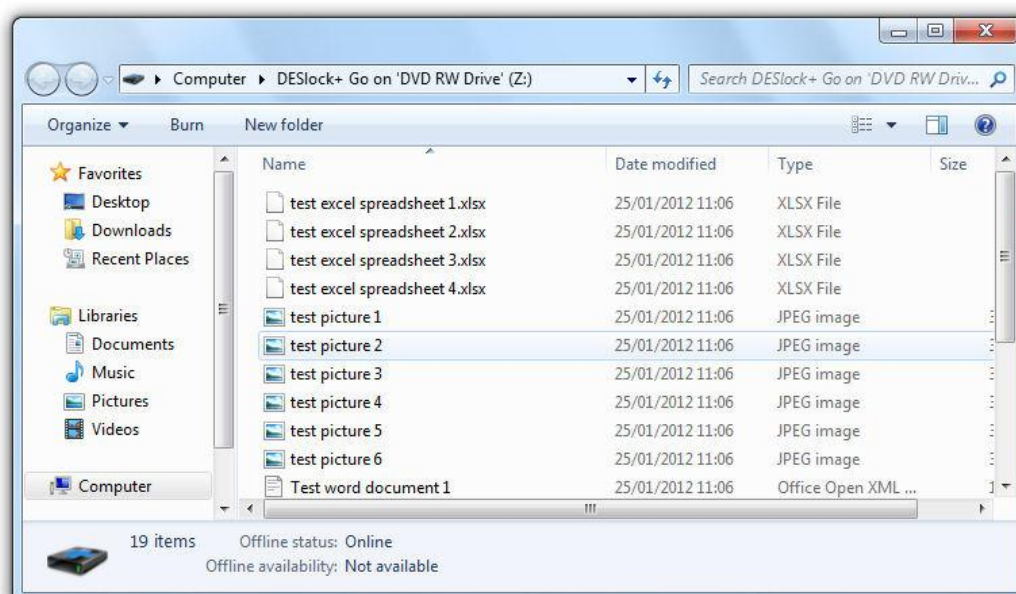


7. You will have 3 password attempts, before the Disc has to be removed and re-inserted into the drive
8. Once the correct password is entered, DESlock+ Go starts, then briefly displays the drive letter assigned to the Disc - next to the system tray. The DESlock+ Go Icon is also placed in the system tray allowing you to exit and secure the drive.





9. Windows Explorer will open automatically giving you access to the Data. Alternatively, you can manually open Windows Explorer and open the encrypted drive letter (in this case drive Z: was assigned).



10. Data on the Disc may then be accessed and opened as normal. Note, there is read only access to this data, any changes must be saved locally, they cannot be saved to the CD/DVD.
11. Once you have finished accessing the data, ensure that the Drive is secured - this will mean that no further access can be made without entering the Password. To do this, click the DEslock+ Go icon in the system tray and select 'Exit & Secure Drive'.



12. Note, on windows 7 systems, the System tray Icon may be hidden - in this case click the Up arrow to the left of the system tray to show the additional Icons.

Full Disk Encryption

DESlock+ Full Disk Encryption allows an entire disk or disks, or selected partitions, to be encrypted using 256-bit AES encryption.

Overview

DESlock+ Full Disk Encryption can be used in two ways, unmanaged and managed. In **unmanaged (standalone) mode** the full disk encryption process and system policies are controlled by the user on the local machine. In **managed (administrative) mode** the full disk encryption process, machine and user policies are set and controlled by the DESlock+ Enterprise Server software.

For users not under administrative control full disk encryption will, by default, run in unmanaged standalone mode. In this mode, the user can choose their own username and password, but there is no built in recovery facility. Because of this, users **must** make careful note of all user and administrative passwords used as if these are lost the system will become inaccessible and the data stored will be lost.

For users who are under administrative control full disk encryption will, by default, run in managed administrative mode. In this mode, using the DESlock+ Enterprise Server an administrator can specify settings for individual machines, including default passwords, but can also securely delegate the process of encryption to the users if required. Additional benefits of using the Enterprise Console include the ability to manage the full disk encryption process and to maintain recovery information to allow access to encrypted machines should user password information be lost.

Before you can use the full disk encryption feature, you must have an appropriate licence.

The time taken to fully encrypt a hard drive depends on its capacity and the other processes running on the machine at the time. Disk encryption typically takes in excess of 1 hour

Note.

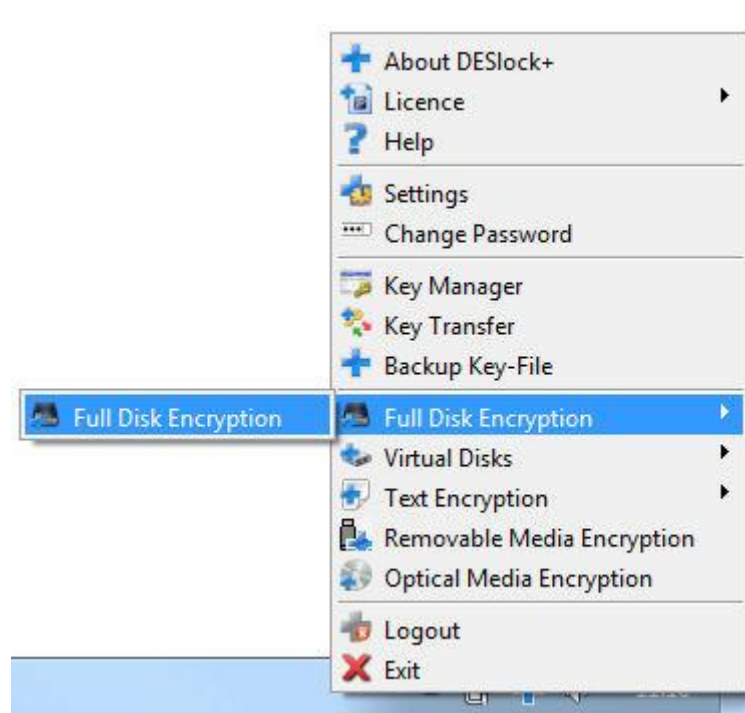
Even though all data on the disk is encrypted, DESlock+ will still allow the further encryption of files, folders etc using encryption keys. This allows the user to safely exchange encrypted data with other users.

Standalone Mode

Unmanaged (Standalone) Mode

If you choose to use the full disk encryption feature you will still be able to work normally whilst the encryption is in progress. You can also shut down and restart your PC, encryption will resume on restarting until completed.

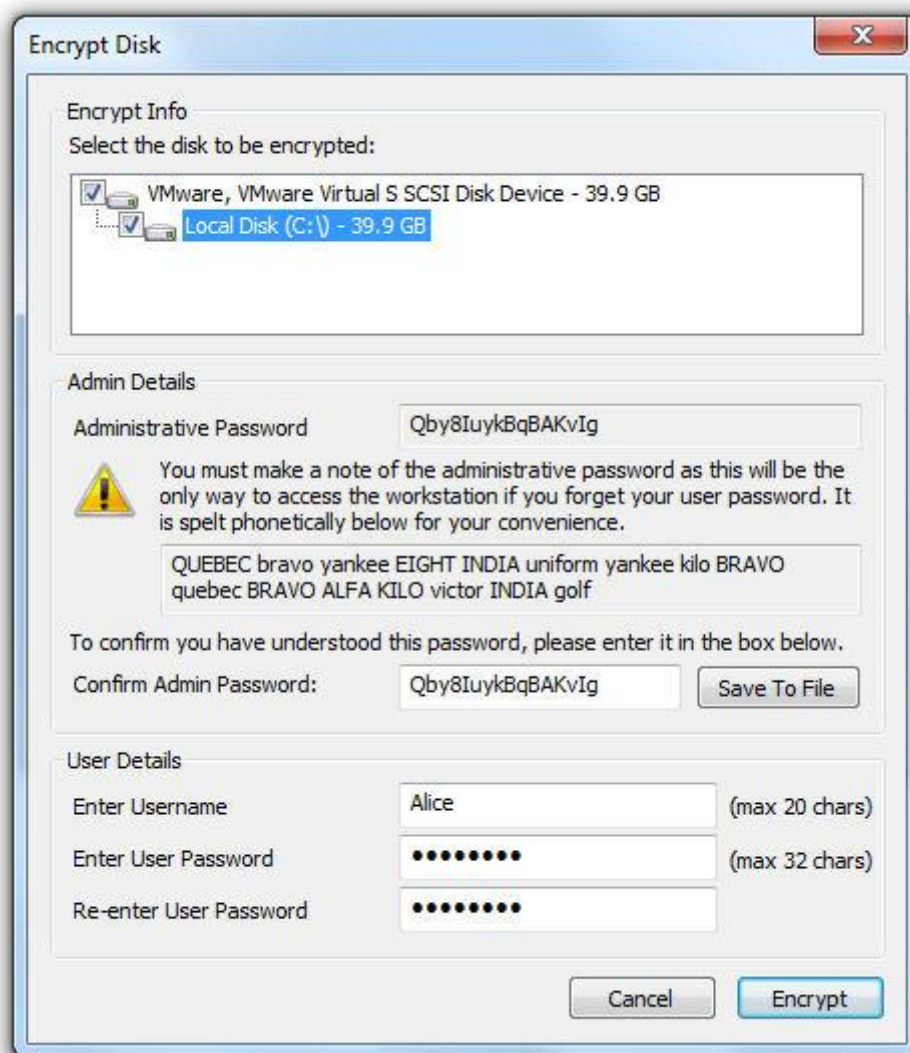
To begin the full disk encryption process, click on the DESlock+ tray icon in the bottom right hand corner of your screen and select 'Full Disk Encryption'.



Next, select 'Disk Management'



Next, select the disk and or partitions you wish to encrypt using the selection boxes.



Refer to the important notes below before continuing.

A randomly generated administrative password is created and shown in the Encrypt Disk window (above) this is also spelt phonetically using the standard NATO/ICAO phonetic alphabet.

Confirm the password by typing it in the box provided. Before proceeding you must save this password using the 'save to file' button. The password must be saved to external storage such as an external hard drive, memory stick or CD. It is also advisable to write this password down and store it securely. If you save the password to an encrypted location you will not be able to access it to recover your Hard drive, as the encryption keys will be located on your hard drive.

Next enter your own chosen username and password for your user account. This is the user name and password that will be required to log into your PC once full disk encryption has been completed.

Again, it is VERY important that you remember both the user name and password, as without them you will be unable to access your PC once it has been encrypted. As a standalone user there is no recovery facility and your system and data will be completely inaccessible.

The user password can be modified at a later date if required.

Click 'Encrypt' to start full disk encryption, then see [Encryption Progress](#) for more detail.

Important notes.

Administrative password.

- Do not save this password to the Hard Disc drive you plan to encrypt.
- Do not save this password to other encrypted media (external HDD, USB memory stick, CD etc), or media that you may encrypt later. Saving to encrypted media is ok, just not media encrypted with YOUR key-file (which will be encrypted on your hard disk, so if you forget your password to your hard disk you cannot get to your recovery password)
- You may save this password to media encrypted with [DESlock+ Go](#) using a password - but it is vital that you do not forget that password.
- IT IS VITAL THAT THIS PASSWORD IS RETAINED AS IT WILL BE REQUIRED SHOULD YOU WISH TO DECRYPT YOUR DISK IN THE FUTURE.

User name and password.

- If you lose or forget the Full disk user name and password you will not be able to access your encrypted drive.

The important point here is to remember that your passwords are like the spare key to your safe - if you keep it inside the safe, it won't help you if you lose the main key. If you forget or lose the passwords to your encrypted information, anything that is encrypted is inaccessible - which will include your password backups if you disregard these warnings.

Managed Mode

Managed (Administrative) Mode

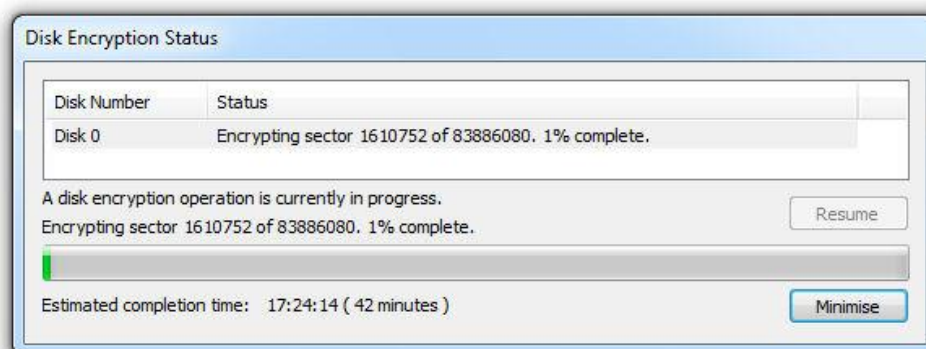
In this mode workstations and users are managed using the DESlock+ Enterprise Server software. This software allows a system administrator to remotely manage encryption features and encryption policy on each workstation and for each user. The Enterprise Server gives the administrator the ability to manage the full disk encryption process and to maintain recovery information to allow access to encrypted hard drives should user password information be lost. Full disk encryption can be started on a workstation remotely and without user input.

If you are a new managed user you will have set up your user password and logged in successfully as described in the section [Login to DESlock+ - Managed Users](#)

If your system policy has been set to implement full disk encryption on your workstation this process will start automatically under the control of the Enterprise Server. You may briefly see a message box above the task bar showing that your system has been updated by (synchronized with) the Enterprise Server followed by the start of the full disk encryption process.



System updated message



Full disk encryption started / progress message

See [Encryption Progress](#) for more information on monitoring the status of the encryption process.

Please see [Login](#) for details of how to login to full disk encryption when starting your PC.

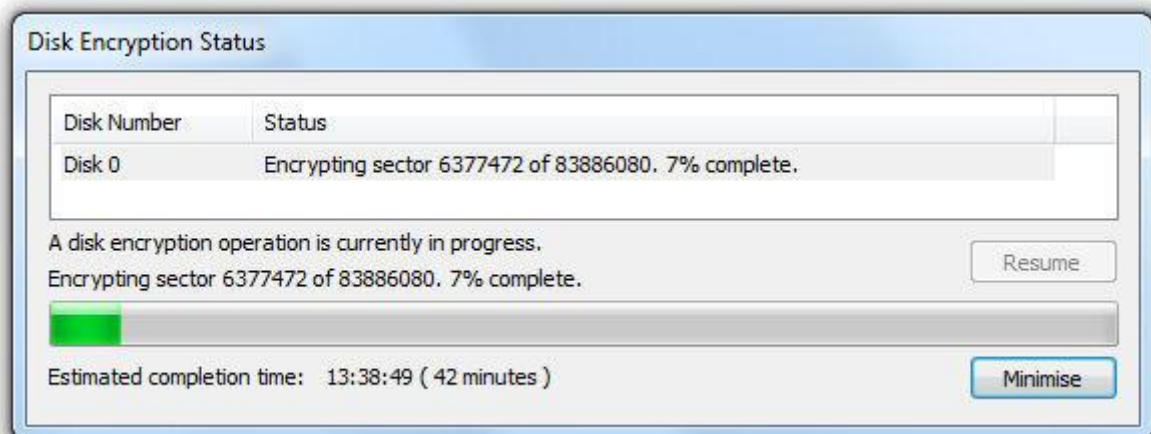
Encryption Progress

Once the full disk process has started a new icon will be displayed in the system tray to indicate that encryption is in progress.



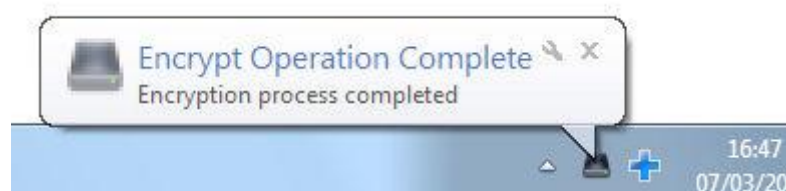
Encryption progress icon

Double clicking the icon will display more details and an estimated time for completion. (This may take a few seconds to calculate). Please be aware that other activity on the machine can affect the speed of full disk encryption.



Disk encryption status bar

The status bar can be minimized and you can also shut down and restart your PC while the encryption is in progress, encryption will resume on restarting the machine until completed. Once encryption is complete a balloon and the progress dialog will indicate that encryption is complete.



Disk encryption completed message



Disk encryption status

Please see [Login](#) for details of how to login to full disk encryption when starting your PC.

Login

Login to an Encrypted System

Once a PC is encrypted or partially encrypted using full disk encryption a new boot screen will be displayed at start up.

To start the system normally, select the first option by pressing return.



Login to a full disk encrypted system

Next enter your chosen username, click return and enter your user password. These are the user details you entered when setting up full disk encryption (see [Standalone Mode](#))

After you have entered the details the PC will boot and operate as normal.

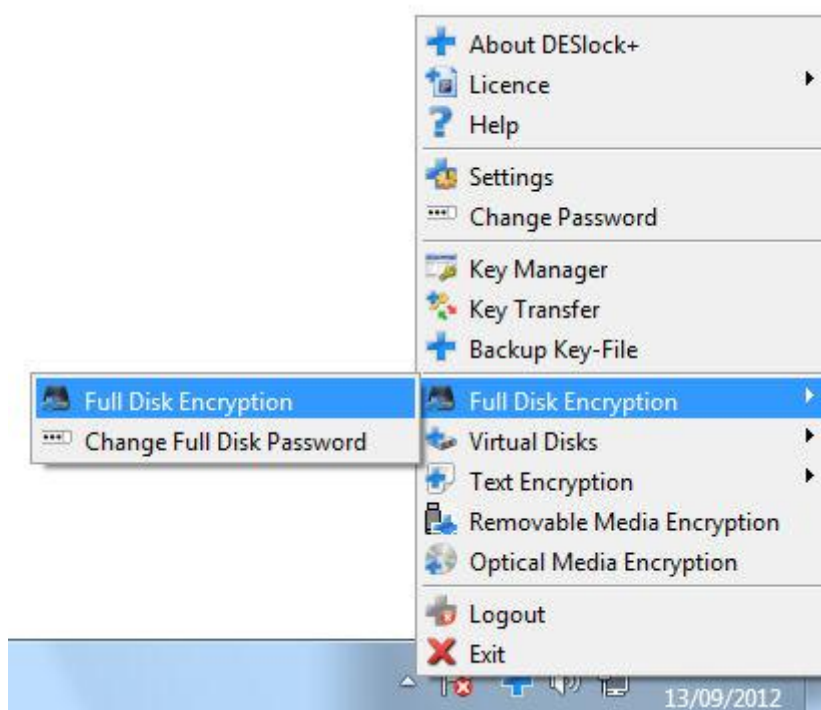


Full disk encryption login, username and password

Managing an Encrypted System

On a standalone, (unmanaged) system that has been encrypted or is partially encrypted, the DESlock+ full disk encryption tool allows user management functions such as adding and removing users. First click on the DESlock+ tray icon in the bottom right hand corner of your screen and select 'Full Disk Encryption'.

If you are working in a managed (administrative) environment, some of the full disk tools may not be available as the policy for workstations and users is controlled by the Enterprise Server software.



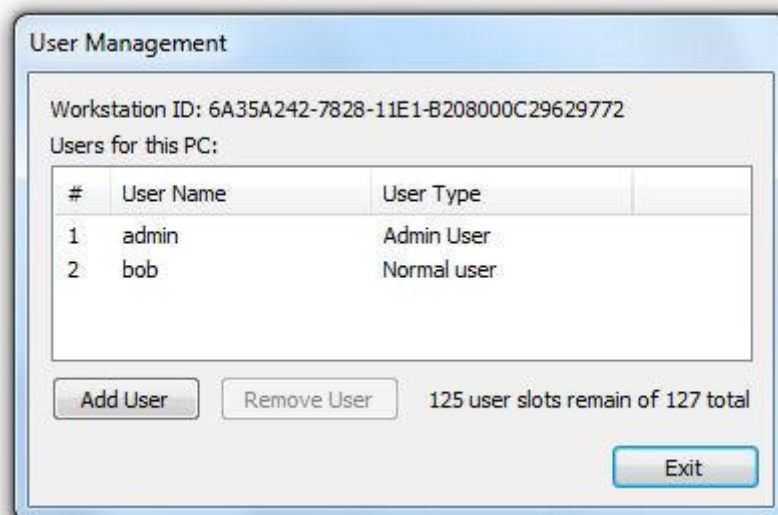
The full disk encryption tool window will open.



Full disk encryption - User App

User Management

Clicking the User Management button will take you to the user list. This displays all user accounts on the local PC. Here you can add and delete user accounts.

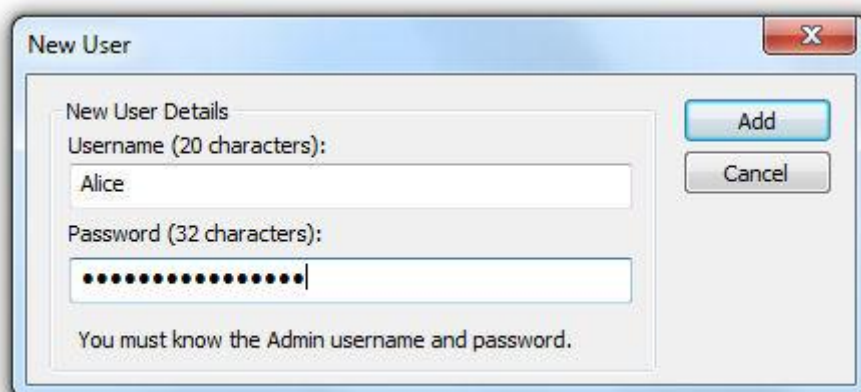


Full disk encryption - user management

Adding Users

You can add up to a maximum of 127 users to an encrypted system. To be able to add a new user you will need the full disk encryption (admin) password. This is the password generated when full disk encryption was applied. See [Standalone Mode](#)

To add a new user, click the 'Add' button. Enter a username and a chosen password. The username can be up to 20 characters long and the password up to 32 characters.



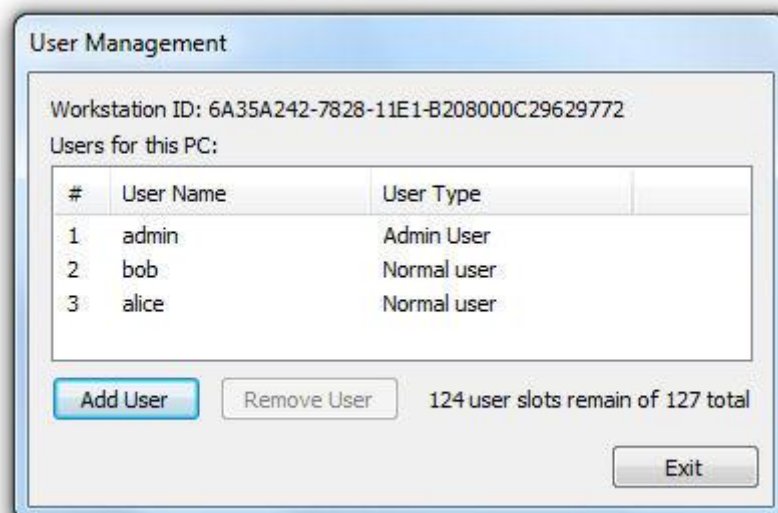
Full disk encryption - add new user

When clicking 'Add', a dialog will appear prompting for the full disk encryption (admin) password. Enter this and click 'Add User'.



Full disk encryption - enter admin. password

The new user will appear in the user list.

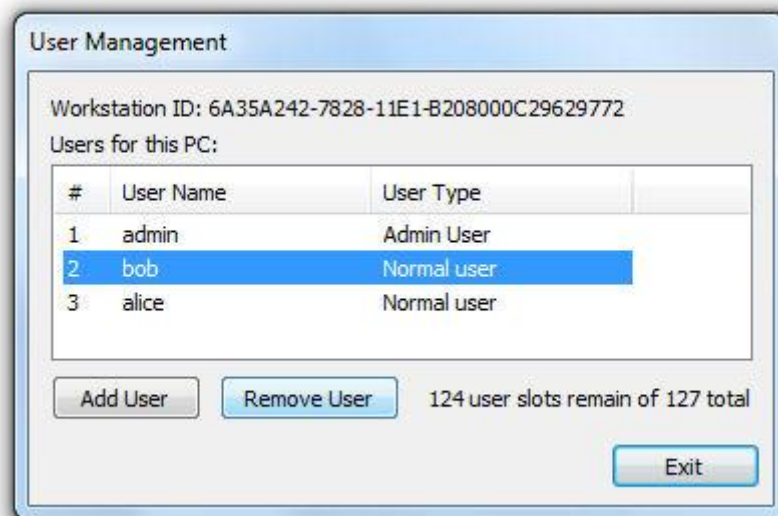


Full disk encryption - workstation user list

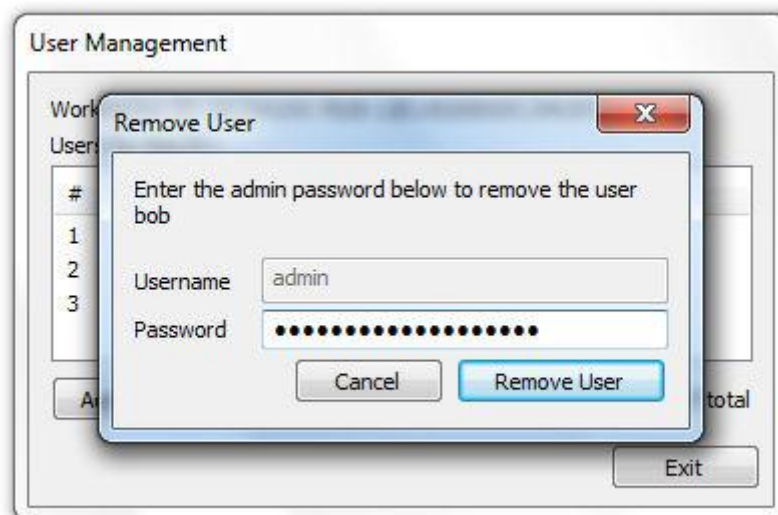
Removing Users

To be able to remove a user you will need the full disk encryption (admin) password. This is the password generated when full disk encryption was applied.

To remove a user, highlight the user, then click the 'Remove User' button.



Full disk encryption - remove user

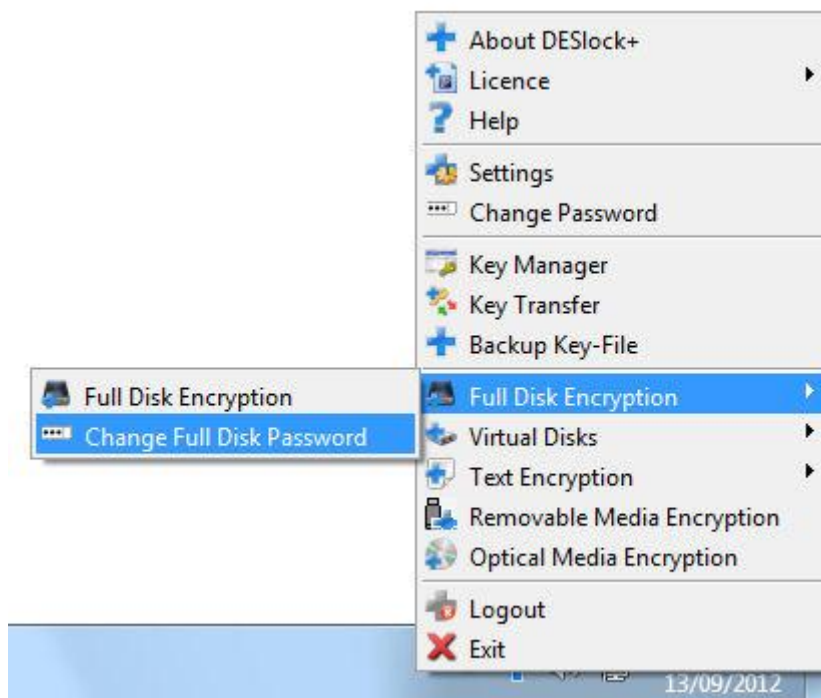


Full disk encryption - enter admin. password

A dialog will appear prompting for the full disk encryption (admin) password. Enter this and click 'Remove User'. The user will then be removed.

Change full disk encryption user password

Only the user is able to change their password. To change the password, right click the system tray, and select 'Change Full Disk Password'.



Full disk encryption - change password

Enter the current password, followed by the new chosen password (twice) where prompted. Then click 'Change' - note, if either the original password is wrong, or the new password and confirmation don't match, the 'Change' button will not be available. If needed, tick the box marked 'Show Typing'



Full disk encryption - enter new password



Full disk encryption - user password changed

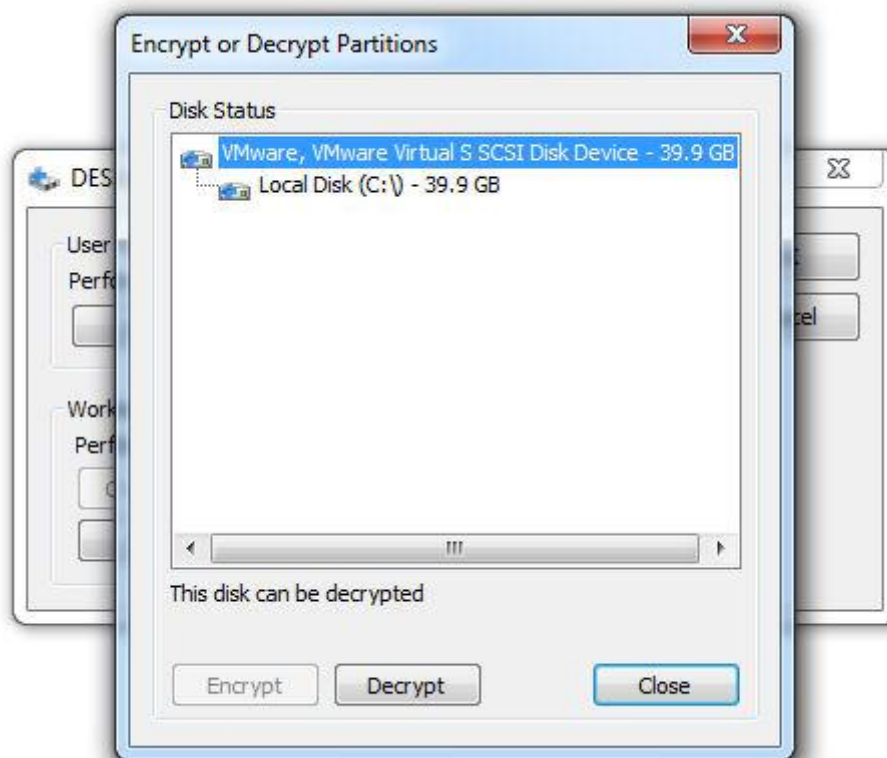
Decrypting

If you click 'Disk Management' when a disk is encrypted, a dialog will be displayed allowing you to decrypt a disk or partition. Alternatively additional disk or partitions can be selected and encrypted. To carry out either operation you will need the full disk encryption (admin) password. See [Standalone Mode](#)



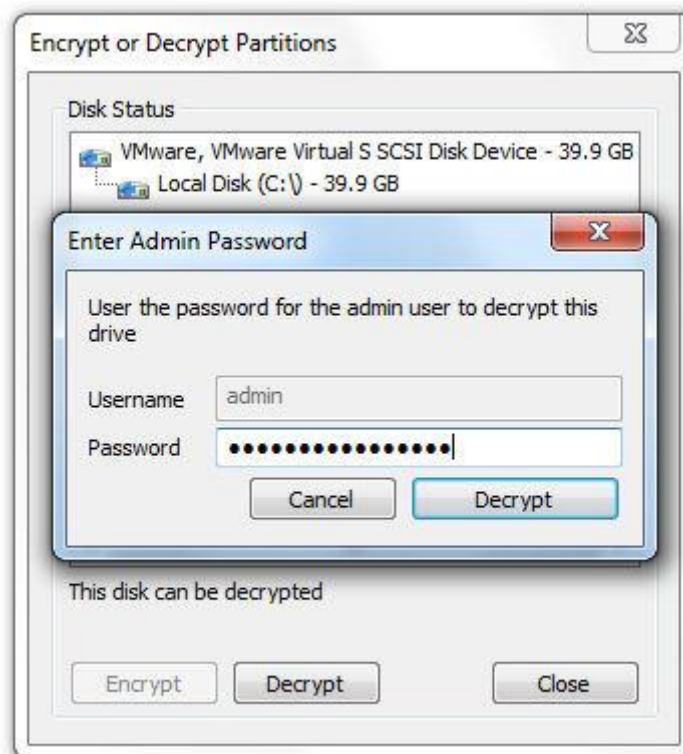
Full disk encryption - disk management

Select the disk or partition you wish to decrypt and click 'Decrypt'



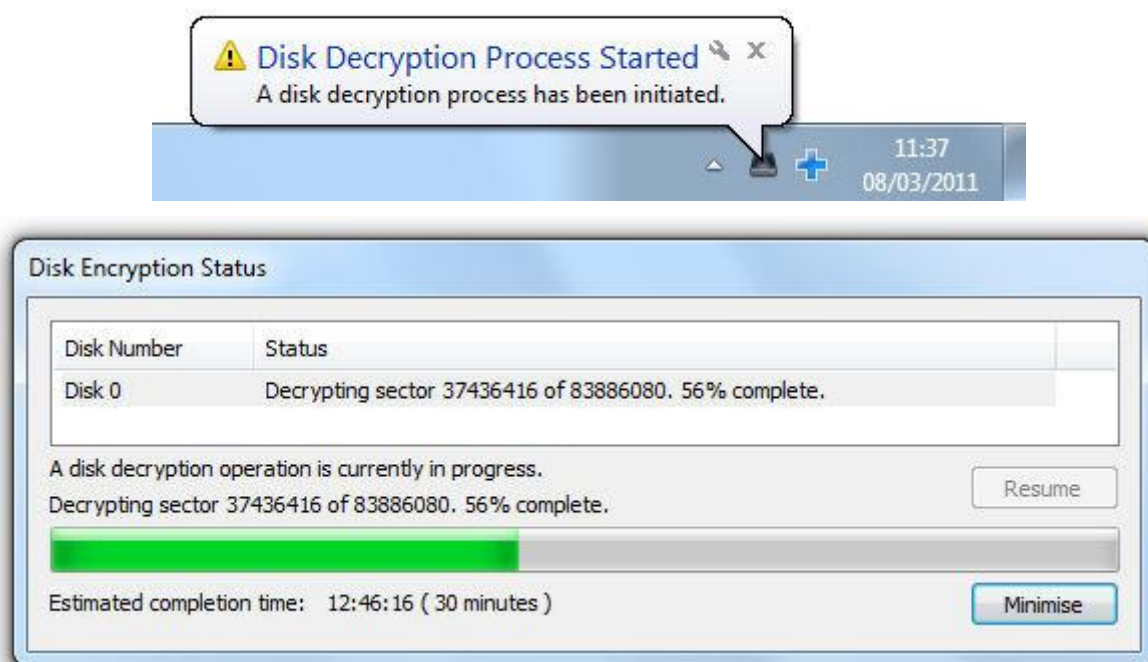
Select disk or partition to be decrypted

Enter the full disk encryption admin password. Click 'Decrypt' to start the process.



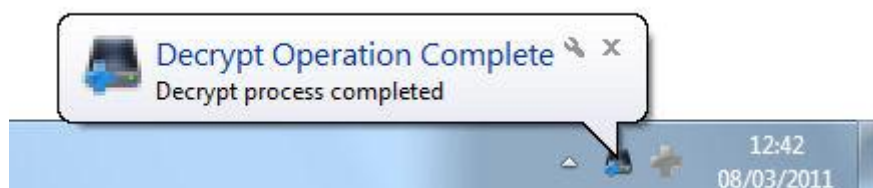
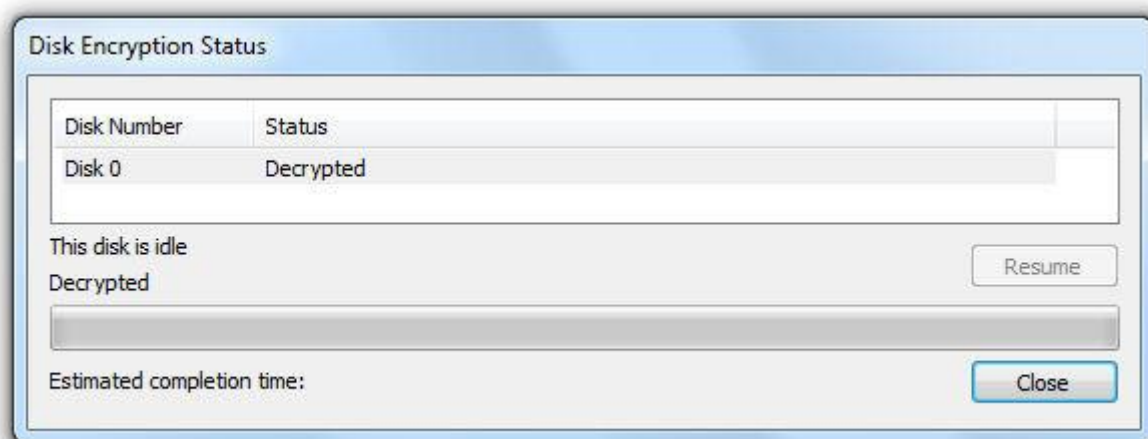
Enter full disk encryption password

A balloon message and a decryption progress window will appear showing the estimated time to complete decryption. The time taken to decrypt a hard drive will depend on its capacity and the other processes running on the machine at the time. Disk decryption typically takes in excess of 1 hour.



Decryption progress window

Once encryption is complete a balloon message and the progress window will indicate that decryption is complete.



Decryption status window and message balloon

Utilities

DESlock+ includes a set of utilities to simplify tasks and to provide the user with more methods to protect their data. These include:

- [Shredder](#) - Secure deletion of data, preventing the "recovery" of deleted files through the use of file rebuilding programmes.
- [DESlock+ Go](#) - In conjunction with removable and optical media encryption, DESlock+ Go allows DESlock+ to be used on a computer without DESlock+ installed.
- [Outlook Plugin](#) - Provides encrypted emails, and also simplifies the key transfer process via email.
- [DLP reader](#) - Allows the decryption of password protected text and files with a simple utility.

DESlock+ Shredder

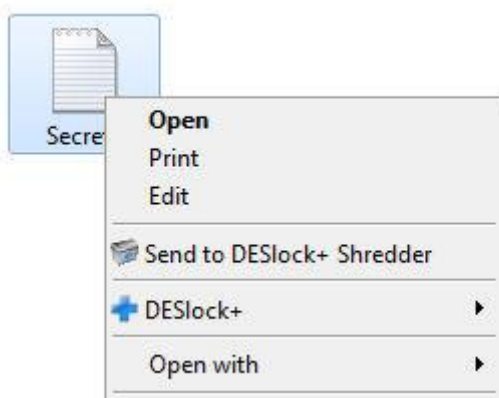
The DESlock+ Shredder allows secure deletion of any file on the computer. The DESlock+ Shredder is accessible via an icon on the user's desktop (below).



DESlock+
Shredder

Shredder icon

Files may be shredded directly by dragging and dropping them onto the DESlock+ Shredder icon. Alternatively, right clicking on a file will bring up the context menu from where the file may be shredded.

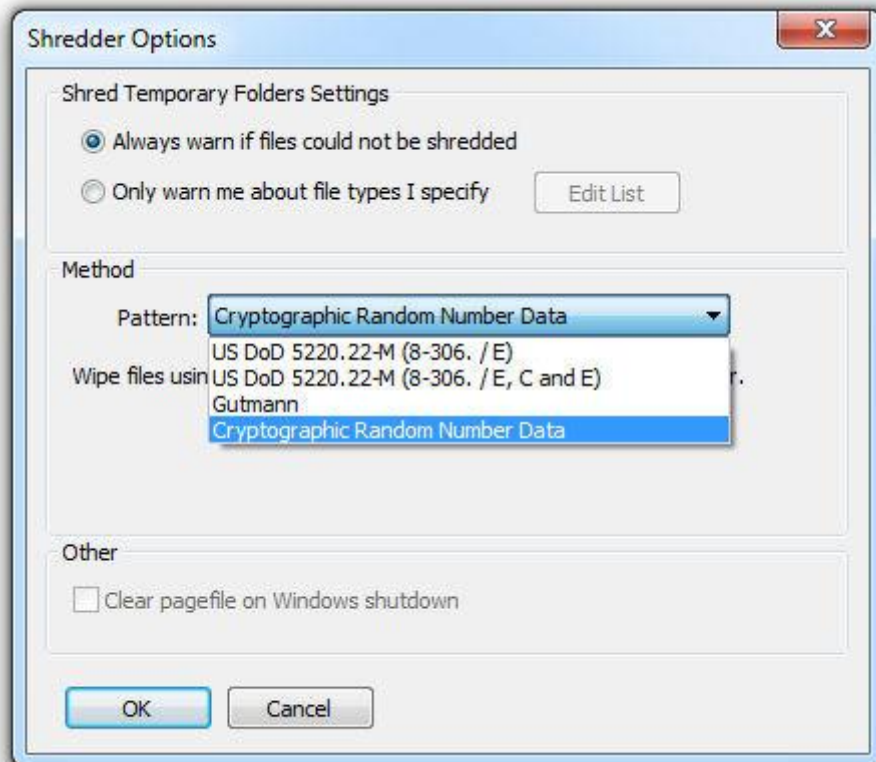


Shredder context menu

DESlock+ Shredder settings allow the user to choose the warning level when shredding files. As some temporary files may be locked open at the time of shredding, unnecessary errors may be received. This general warning on any file can be modified to only warn about specific file types.



Shredding options



Shredder settings

The DESlock+ Shredder may use one of four methods to shred files. Either writing a cryptographically secure random number stream over the file; the Gutmann method, or using the US Department of Defence 5220.22-M standard for sanitising data (two different passes available). On modern hard disks there is no benefit to using the DoD standard as all the methods would destroy the data equally as well and using cryptographically secure random numbers is faster.

DESlock+ Go

DESlock+ Go allows you to use an encrypted removable device (Removable or Optical Media) on a PC without DESlock+ installed. In order to use this feature, the device must be encrypted with file level encryption with an encryption key and a DESlock+ Go Password. The device will be accessible as usual on any DESlock+ enabled PC (i.e. only accessible if you have the correct encryption key), and using the DESlock+ Go password encrypted data will be accessible on any PC.

To use DESlock+ Go with a removable media device (USB memory stick):

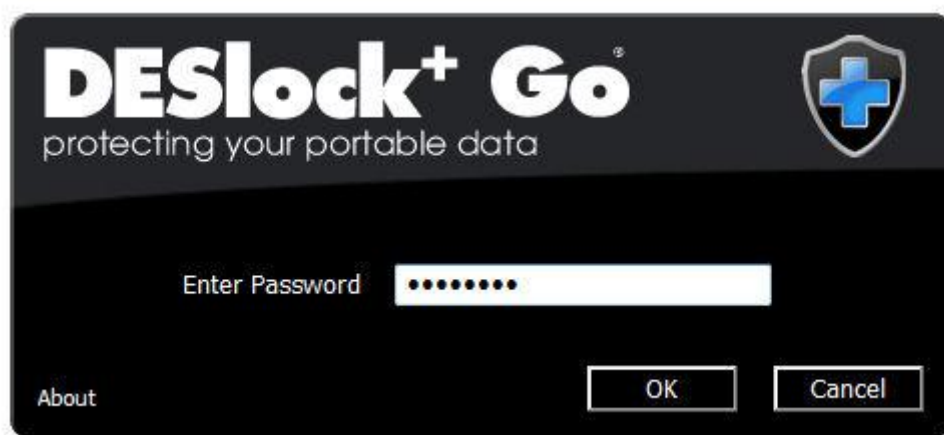
1. Encrypt a memory device (right click the DESlock+ System tray Icon, select "Removable Media encryption") - for more details on this see [Removable Media File Mode Encryption](#)
2. Select the Removable Media Device from the list and click 'Encrypt'.
3. Select 'File' type encryption.
4. Select the required encryption key then define the DESlock+ Go password.
5. The Removable media device will now be set up with an encrypted folder and the DESlock+ Go program copied to the drive. In use, any file copied to the encrypted folder will be available to any person knowing the password and to any DESlock+ user with the correct encryption key.
6. Any file outside the 'Encrypted' folder will NOT be encrypted.



DLP Go on a PC without DESlock+

Using on a machine without DESlock+

When inserting the device, the Auto Run should launch the DESlock+ Go executable. Enter the password that was configured earlier.



DESlock+ Go password use

If Auto run is not enabled, navigate to the device and start DESlock+ Go by double clicking on DLPgo.exe in the root of the device.

If the password is entered correctly, the encrypted portion of the drive will become accessible as a separate drive.



DESlock+ Go drive available

The DESlock+ Go drive will be shown in My Computer with the following icon and description.

Devices with Removable Storage



3 1/2 Floppy (A:)



DVD-RAM Drive (D:)



Removable Disk (E:)

Network Drives



DESlock+ Go on 'Removable Disk'
(Z:)

My Computer DESlock+ Go Icon

DLP Go on a PC with DESlock+

Using on a machine with DESlock+

An additional benefit of DESlock+ Go is that the DESlock+ Go password can also be used to access the drive on a system that has DESlock+ installed but for which the Key-File does not contain the correct encryption key.

When the device is inserted and the encryption key is not found, the user will be prompted for the password to access the device. Enter the DESlock+ Go password and access the drive as normal.



DESlock+ Go use in existing system

Outlook Plug-in

The DESlock+ Outlook Plug-in is designed to integrate with Microsoft Outlook 98 or later to provide DESlock+ encryption of emails and email attachments.

If Outlook is not being used, email messages and attachments can still be manually encrypted to retain security. Please refer to the [Text Encryption](#), [Archives](#) and [File Encryption](#) documentation.

Note. DESlock+ requires that Word is not selected as your email editor, which is an option available on early versions of Outlook (98-2003).

To do this, from the Outlook Tools menu, select Options and on the Mail Format tab uncheck the "Use Word when editing e-mail messages" check box.

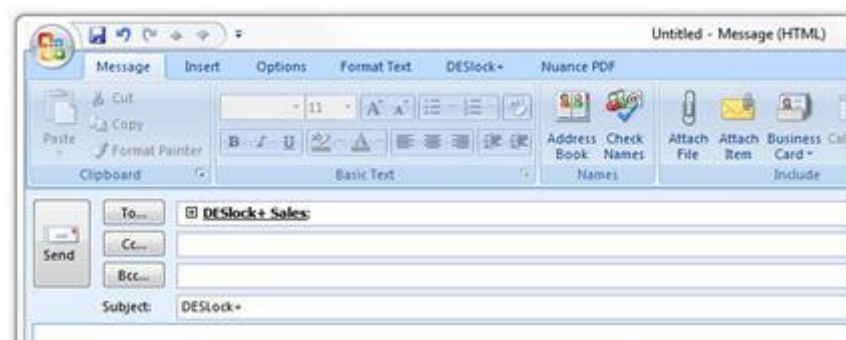
Outlook 98-2003

Outlook 98-2003 Integration

When installed, the Outlook Plug-in will add a DESlock+ menu to the menu bar and a DESlock+ icon (below) to the toolbar of the main Outlook window (below).



DESlock+ tray icon



Outlook message DESlock+ toolbar

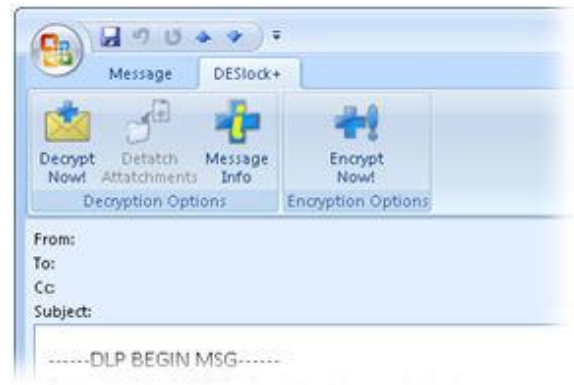
Outlook 2007

Outlook 2007 Integration

If using Outlook 2007 with the DESlock+ Outlook 2007 add-in, this will add new icons to ribbon bars of the compose and read forms within Outlook.



Compose form








Read form

Aside from these visual differences the operation of the add-in is identical to that with Outlook 98-2003.





Email Options

Each Outlook email message window may contain the icons listed below which provide additional email options. The options are also available from the DESlock+ menu in the message window. The appropriate set of options depends on whether the user is the sender or recipient of an email. Some options may be unavailable depending on the mail format.

Sender Options

Icon	Meaning
	Decrypt for Reply: When replying or forwarding a message, automatic decryption of the quoted message is disabled. Click this button to decrypt the previous message. This is only possible if the originator of the encrypted message has not chosen the Force Viewer option.
	Encrypt and Send: Click this button to encrypt the body of the email, including any attachments, and immediately send the email in one action.
	Encrypt on Send: Click this button to encrypt the email body before sending. The email body will not be encrypted until the email is sent.
	Encrypt Now: Click this button to immediately encrypt the email body. The message can be further edited before being sent. Attachments will not be encrypted immediately but 'Encrypt Attachments' can still be used.
	Force Viewer: Click this button to force the recipient of the email to use the DESlock+ Message Viewer , rather than allow the email to be decrypted in place.

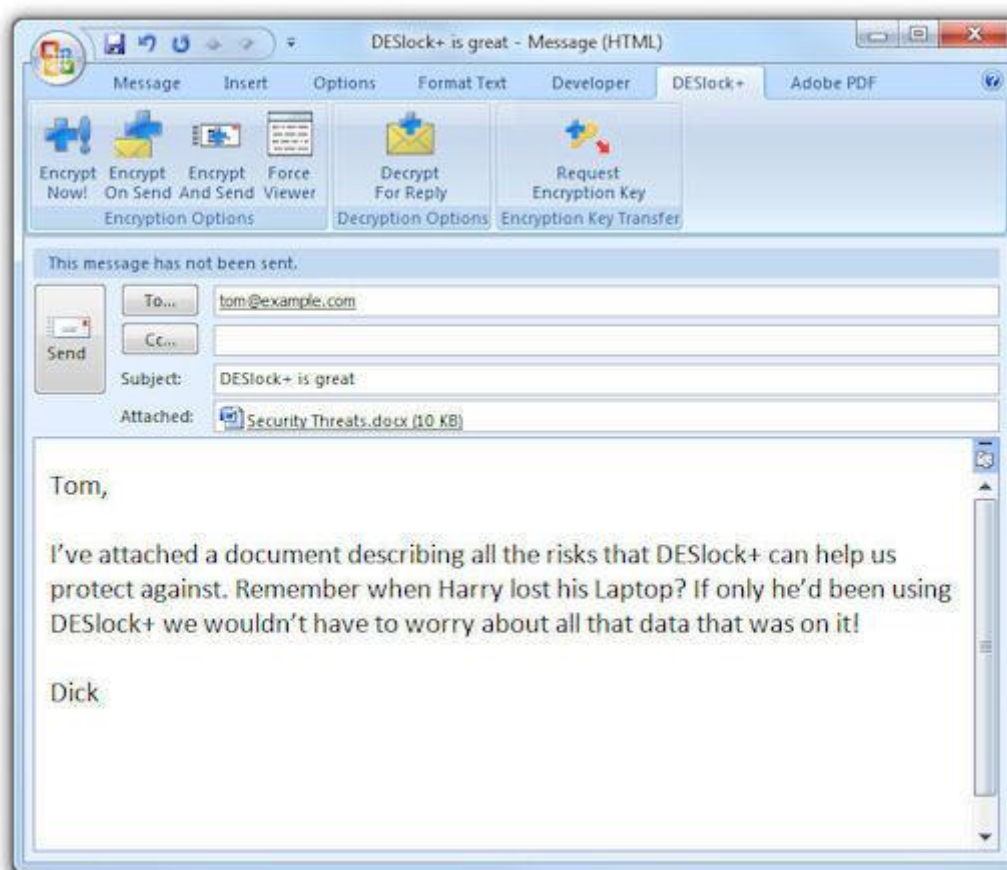
Recipient Options

Icon	Meaning
	Decrypt Now: Click this button to decrypt a DESlock+ encrypted message.
	Decrypt All Attachments: Click this button to decrypt and save all attachments from the email to a user specified folder. The user must then 'browse' to an existing folder in which to save the files.
	Encrypt This Message: Click this button to encrypt any plain text message. This can include any messages received from a user who is not using DESlock+.
	Message Info. Click this button to see the encryption properties of the message.

Encrypting a message

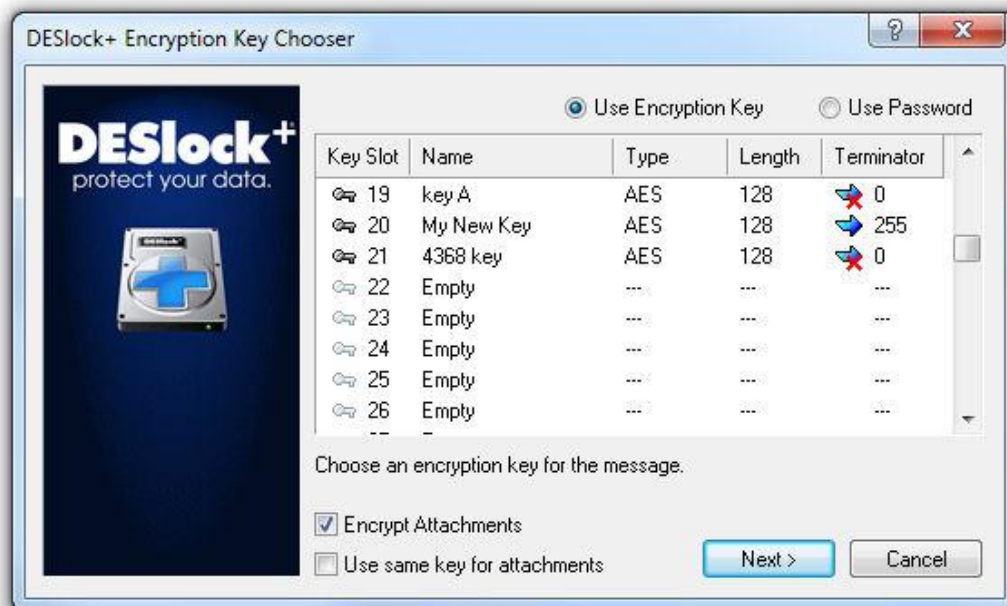
When encrypting a message, the user has three options. To encrypt the email and send it using 'Encrypt **on** Send' or 'Encrypt **and** Send'. Alternatively, the user can use 'Encrypt Now' to encrypt the message and add additional text that can either be encrypted using a different encryption key or can be left in plain view.

In this example we shall choose to encrypt the message and edit it before sending. Below is the original message before clicking the 'Encrypt Now' button.



Outlook message encryption

After choosing to encrypt the message, an encryption key must be selected or password must be set for the encryption of the message. Any user of DESlock+ can decrypt a message encrypted using a password if they know the password. If an encryption key is used then the recipient must have a copy of that encryption key available to them.



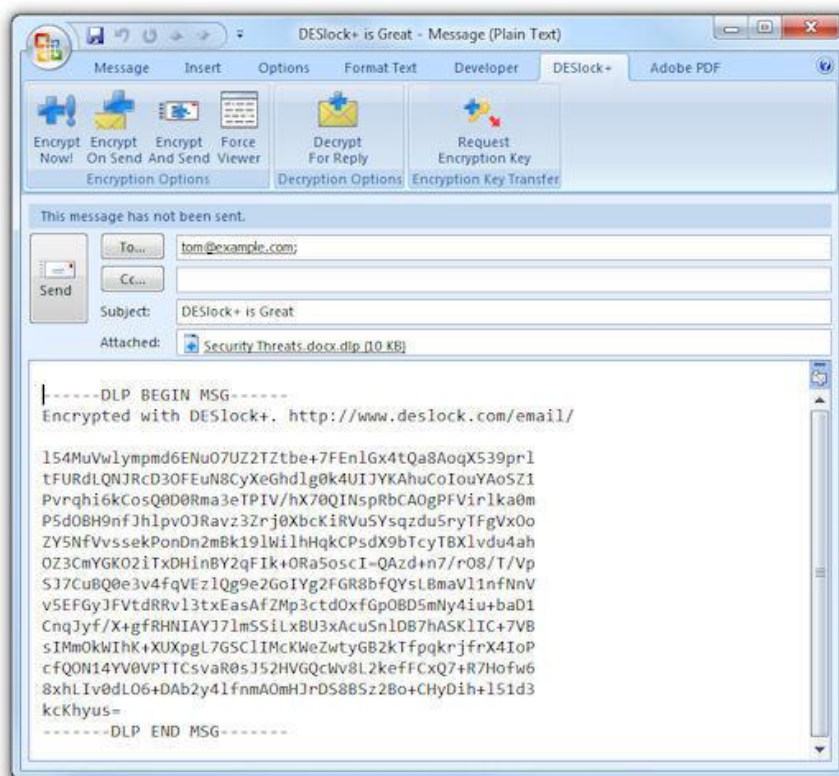
DESlock+ key chooser

If the message has attachments, the option to select a different encryption key to encrypt the attachments is given. If an alternate encryption key is required, uncheck **Use same key for attachments** and choose a second encryption key on the following screen. If a password was chosen above, this same password will also be used to encrypt attachments.



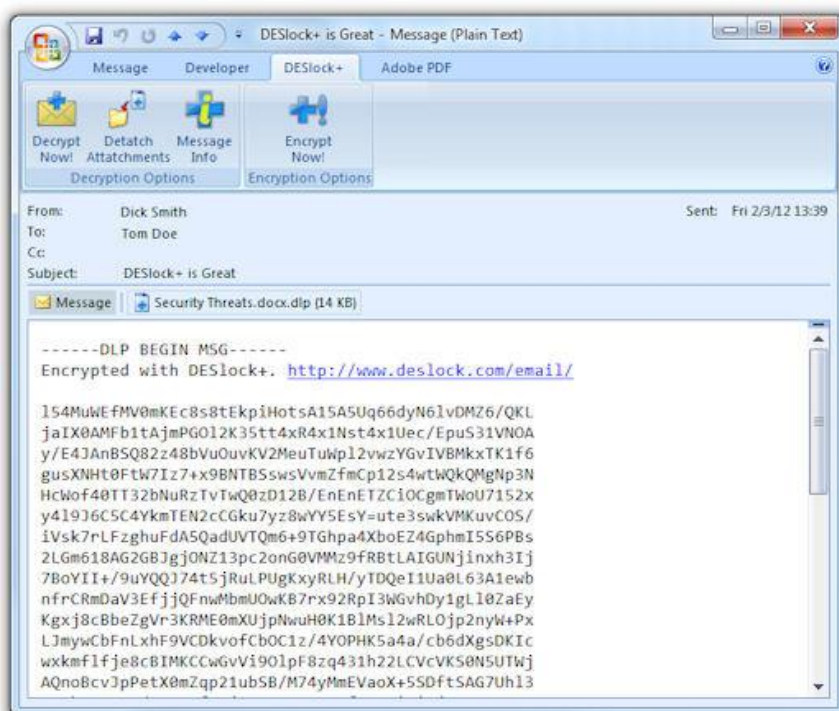
Outlook attachment key choice

Below is the message after encryption. Please note that the message text has been encrypted along with the attachment. Some plain text can now be added to be sent along with the encrypted message. Any additions must be outside the Encrypted section headers and footers.



Encrypted email

Below is the message as the recipient would see it.



Received email

Depending on the setting used, and assuming the recipient has the correct encryption key, the message can be decrypted in the email window or in the [DESlock+ Message Viewer](#).

Message Info

Selecting '**Message Info**' from the **DESlock+** menu will show details of the encryption key used to encrypt any DESlock+ encrypted message. The encryption key serial number and algorithm type will always be displayed. If the encryption key exists within the active Key-File key space, the location (key slot) and key name will also be shown. If the email was encrypted using a password, the text "Uses Password" will be displayed in the Key Name box.

If the encryption key does not exist in the active Key-File key space the option to request the encryption key is given. If the button is clicked an encryption key request email will be generated when the properties dialog is closed. This email will be addressed to the encrypted message originator but this can be changed prior to sending the message if required. The request message can then be sent to the desired user and used by them in the key issue process.



The screenshot shows a Windows-style dialog box titled "Message Properties". It contains a section labeled "Message Encryption" with several text input fields. The "Encryption Type" field contains "3-DES". The "Encryption Key Serial Number" field contains "00000FEB0000". Below these fields is a text label: "Your token has a copy of this encryption key, with the following details:". Under this label, the "Encryption Key Name" field contains "My Key" and the "Terminator Count" field contains "1". An "OK" button is located at the bottom right of the dialog box.

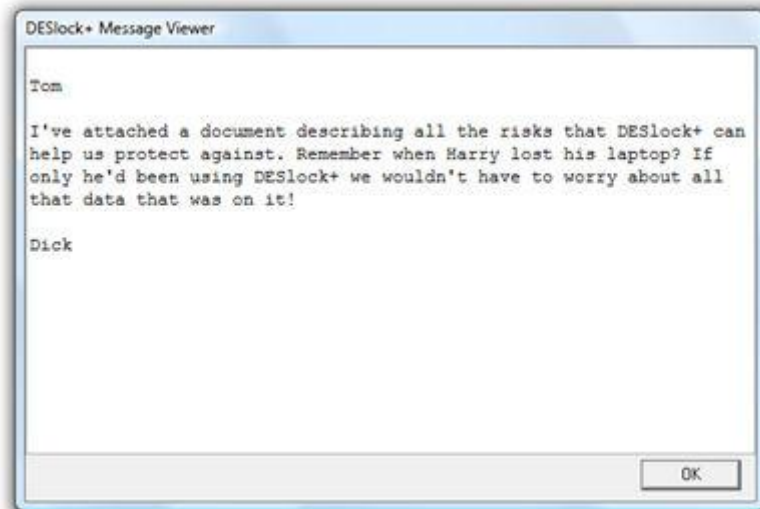
Message Encryption	
Encryption Type	3-DES
Encryption Key Serial Number	00000FEB0000
Your token has a copy of this encryption key, with the following details:	
Encryption Key Name	My Key
Terminator Count	1

Message properties

DESlock+ Message Viewer

The DESlock+ Message Viewer is a simple tool that enables an encrypted message to be viewed securely. When used, DESlock+ will decrypt an encrypted message to the viewer window rather than decrypting the original copy in the email.

The DESlock+ Message Viewer disables any editing of the email including copying the text using Windows clipboard.

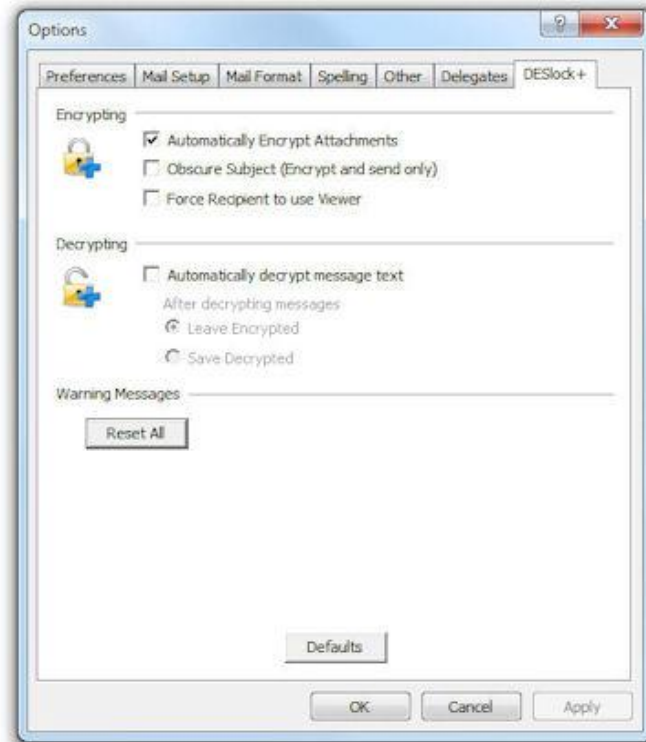


DESlock+ Message Viewer

Even after the message has been decrypted to the viewer, the original email will remain in the encrypted form. A decrypted copy of the email therefore cannot be forwarded if '**Force Viewer**' is selected when encrypting the message.

DESlock+ Configuration

Selecting 'Outlook Tools', 'Options' and then clicking on the DESlock+ tab will display the configuration dialog (below) which allows control of the default operation of the DESlock+ Outlook Plug-in.



Outlook DESlock+ configuration

Encrypting Messages

Automatically Encrypt Attachments

If selected, the Plug-in will default to encryption of email attachments when the message body is encrypted.

Obscure Subject (Encrypt and Send only)

If selected, the original subject field of an encrypted email is replaced with the text "A DESlock+ Encrypted Message". The original subject is encrypted and saved with the message and is only visible after decryption.

Force Recipient to Use Viewer

If selected the recipient of the message will be forced to use the DESlock+ message viewer to view the message, regardless of the recipients DESlock+ viewing options.

Decrypting Messages

Automatically Decrypt Message Text

If selected, any DESlock+ encrypted emails will automatically be decrypted when they are opened assuming the correct encryption key is stored within the active Key-File. If not selected, 'Decrypt Now' must be manually selected.

After Decrypting Messages

Select to either always store the message in encrypted format, even if it has been decrypted, or to store the message in decrypted format after it has been decrypted.

Warning Messages

Reset All

If any of the warning message boxes have been previously dismissed with 'do not ask me again', clicking this button will cause all messages to revert to their initial state so will be displayed until dismissed again.

Key Transfer

In addition to encrypting messages and attachments, the Outlook Plug-in also provides key transfer integration allowing the entire key transfer process to be performed from within Outlook. Refer to the [Key Transfer Wizard](#) section for a more detailed overview of the process.

Three additional options are available depending on the current stage of key transfer. These are listed below.

Request Key

To request an encryption key, **create a new email** message from within Outlook. From the DESlock+ menu of the message window (or Ribbon tab in Outlook 2007) choose 'Request Key'. The message can then be addressed and edited before being sent, at which point a request file will automatically be attached to the email.

Process Key Request

The recipient of the Request email should then choose 'Process Key Request' from the DESlock+ menu of the message window (or Ribbon tab in Outlook 2007). Selecting this will allow the creation of an issue file based upon the attached request file.

An encryption key to transfer must be selected in the same way they would using the [Key Transfer Wizard](#).

When the encryption key has been specified the Plug-in will create a new email containing the issue file and save it to the 'drafts' folder in Outlook. The user issuing the key must open this email, address it and send it.

Process Key Update

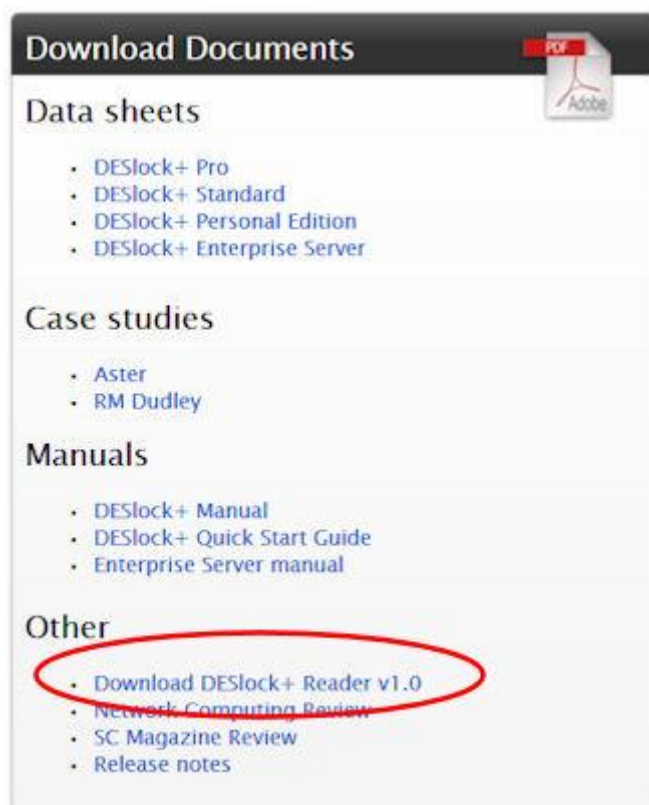
When the user requesting the encryption key receives the update email, they should choose 'Process Key Update' from the DESlock+ menu of the message window (or Ribbon tab in Outlook 2007). This will allow the encryption key to be added to the Key-file key space (See [Update your Keyfile](#)).

DLP Reader

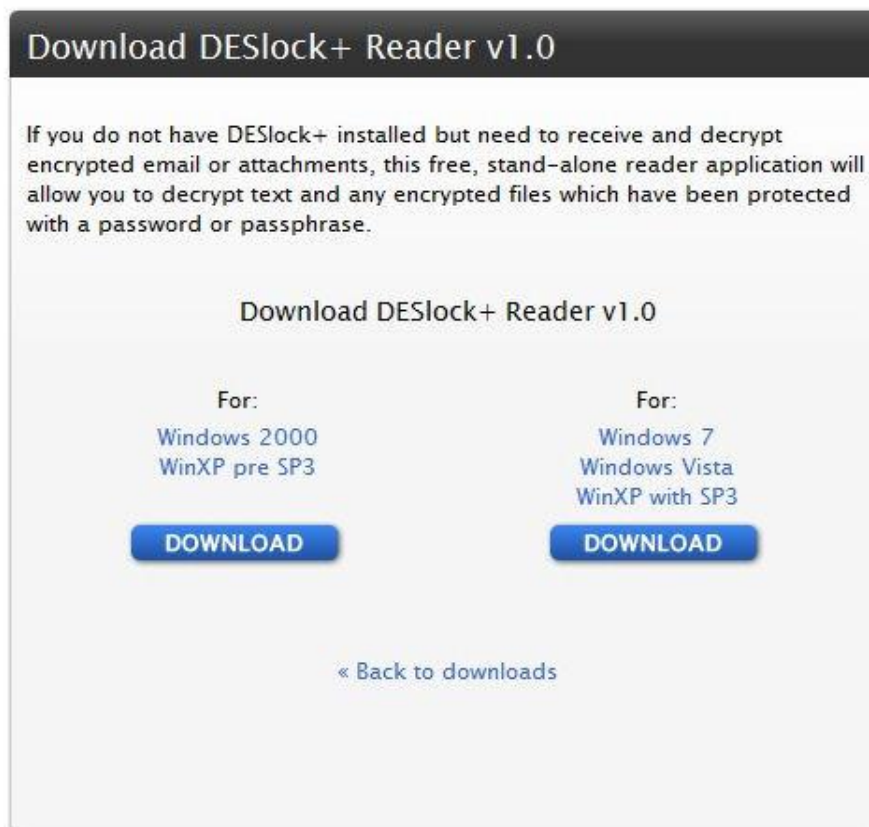
This is a simple utility that allows a licenced DESlock+ user to send Password Encrypted files, mails, or text to a person who does not (or cannot) have DESlock+ installed. This program will allow the decryption of that protected data.

DESlock+ Reader has to be downloaded from the DESlock+ website (www.deslock.com).

Navigate to the downloads page. From the 'Download Documents' panel (on the right hand side of the page) select DESlock+ reader from the "Other" section. As circled below:



Then select the correct version for your operating system



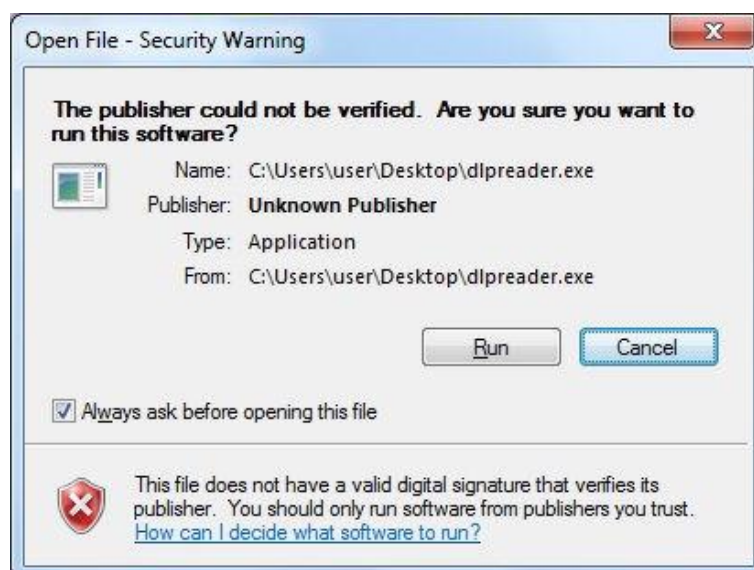
Save the file to a suitable folder on your PC.



Once saved, double click the installed file (with the icon below and named DLPReader.exe) to start the DESlock+ Reader. This utility does not install as a program, and so will not appear in your list of programs (EG windows Start menu, programs). It has to be run by either double clicking or by dropping an encrypted file onto the file icon.



Depending on your Internet browser you may get the following warning, click 'Run' to start the program. If you deselect the "Always ask before...." check box you will not get the warning each time you run the utility.



DESlock+ Reader will now run. The window below can be used to decrypt encrypted files.



To use the DESlock+ Reader all that is required is to either cut or copy and paste encrypted text into the 'Decrypt Text' section of the Reader and click the decrypt button. You will then be prompted to enter the password for the text, and it will be decrypted and displayed. You can also drag and drop encrypted files into the window, enter the password as before and the file will be decrypted. For more details and a step by step guide see [DLP Reader example](#)

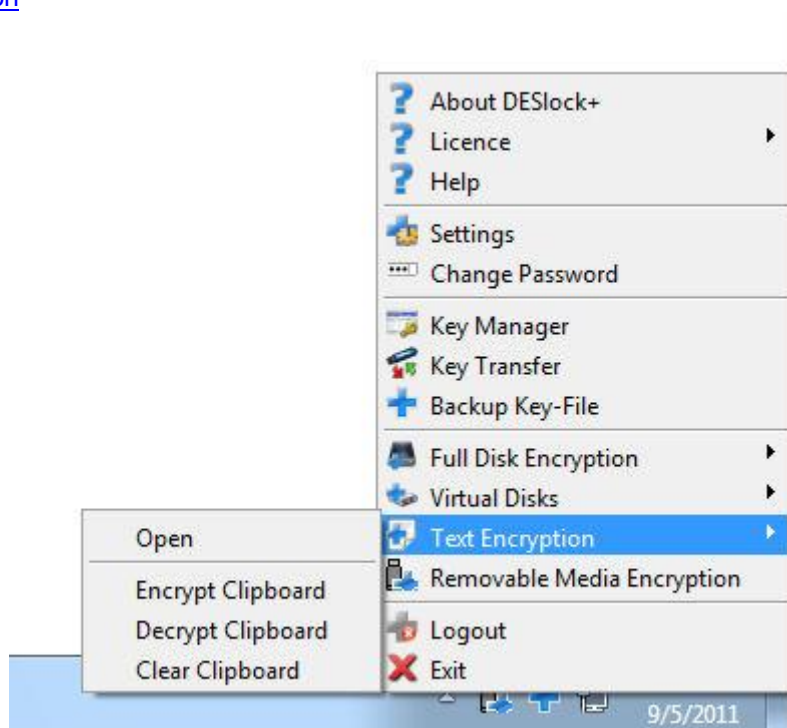
DLP Reader example

As an example, to use DESlock+ Reader follow the steps below.

Licenced User

To encrypt a section of text.

Select the text, right click and copy it. Then right click on the DESlock+ icon in the system tray and use the 'Text Encryption' option to encrypt the selected Text to the Clipboard. For more details on this Utility see [Text Encryption](#)



This will encrypt the text in the Windows clipboard.

Paste the encrypted text into a mail, Text file or word document (or any other program where text can be pasted)

The pasted text will look similar to this:

```
-----DLP BEGIN MSG-----  
Encrypted with DESlock+. http://www.deslock.com/email/  
  
l54Mue9HpbD5+YaWMLyyKs4P+uaAvYOrpV1JhFb/C1vVjnkyLc  
fkChVuZuhyoU407rF3Ci/KuCoyPKzih31sgRwsijMLpohggVW  
HeiCjFW6X0kD44ppk+ggMa9UbGrw3Q4FupxTFB+7J1JlmW78Nt  
RtkvhfVI2ippRjh2JzfacdVatdJ4joDxHYST1TKUnxe7uXjEY2  
qGaUrTKdnMUqh1XCf8XBcn3yGryjzp9/ac2nYs4LiGZPZ72OuZ  
myAwhXHZj6XEu+kydoMWdytSEfq7jQxug=QmMvhBZgXNa0ssE/  
c6T61lwbqQKbG57ovORftSWozSHoS6RMrroXO5f+DDaxYIFCG9  
1YwwkY9qCpfhY0ugG1NrGpl6dXLkIQOJN2qIFIOQ==  
-----DLP END MSG-----
```

Send the document (mail/word etc) to the planned recipient. Tell them independently what the password is. As an example, for the text above the password is "deslock".

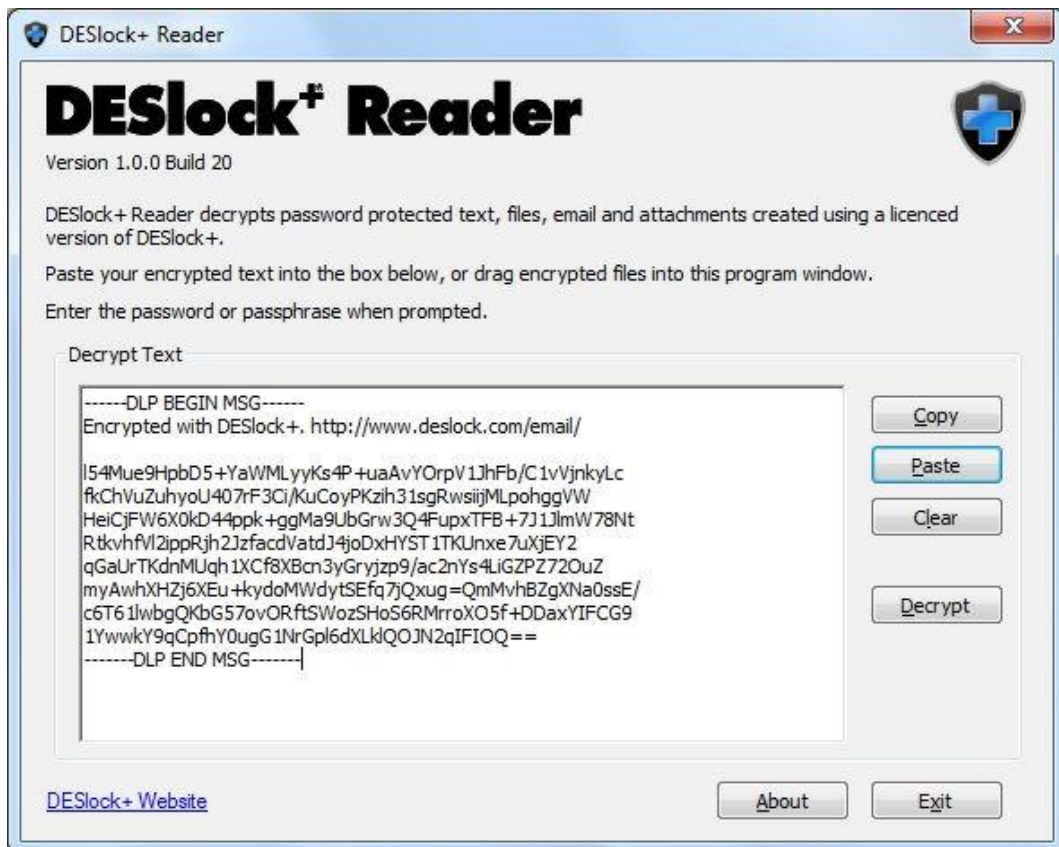
Reader User

Having downloaded the DESlock+ Reader from the website as previously described, start the utility by double clicking on it.

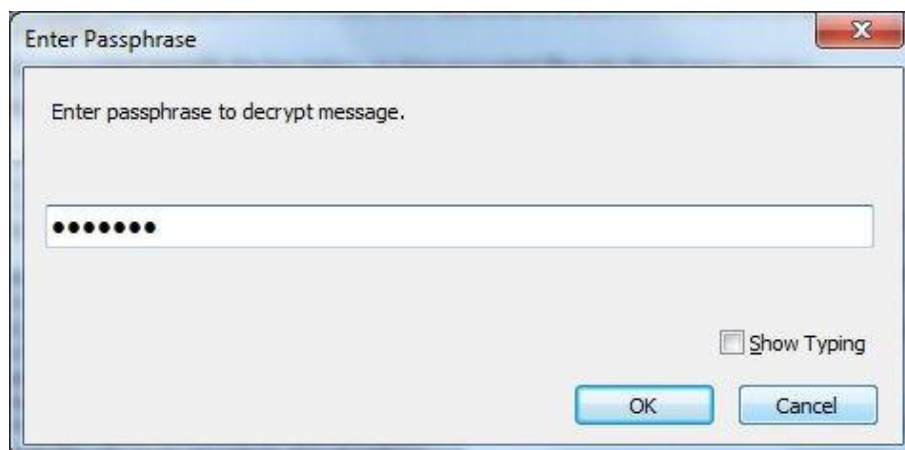
Open the document (text, mail, Word Doc) and copy the encrypted text from it. (highlight the text, right click and copy)

IMPORTANT - make sure you include the -----DLP BEGIN MSG----- and the -----DLP END MSG----- sections in copied portion of the text.

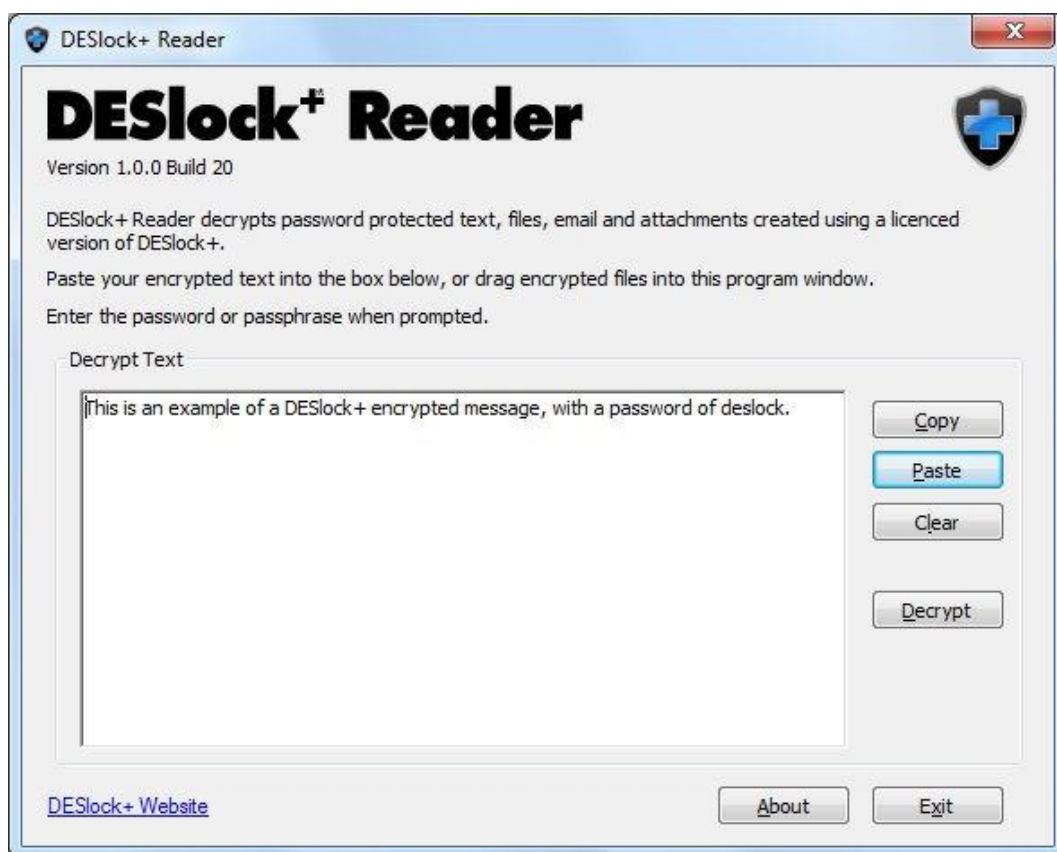
Then paste the copied text into the Reader "Decrypt Text" window. (right click and select 'Paste' or click the 'Paste' button.



When prompted, enter the password or phrase supplied for the encrypted text and click 'OK'.



The text will be decrypted if the correct password or phrase has been supplied and will be displayed in the text window.



Encrypted Files

Files encrypted with a password can also be decrypted using the DESlock+ Reader. To do this, right click the file, select 'Encrypt with DESlock+' and instead of choosing an encryption key, a password should be selected (check box). For more details on encrypting files with DESlock+ see [File Encryption](#)

If an Encrypted file has been supplied, it can be dragged and dropped into the Decrypt window, then you will be prompted for the password. The file will be decrypted and a copy of the decrypted file will be saved in the same folder/location as the original.

Support links

If this help file has not answered your question, or you are still unsure of how to use DESlock+, or you have an unresolved problem or questions, please select one of the links below:

- www.deslock.com - General information, new versions, press releases.
- [eSupport](#) - To resolve Technical issues, or for more detailed information on the product.
- [Knowledgebase](#) - To search our existing knowledgebase of useful articles.
- [DESlock+ Sales](#) - To Email our sales team.